COMPUTERS IN EDUCATION: LEGAL LIABILITIES AND ETHICAL ISSUES CONCERNING THEIR USE AND MISUSE

By Patricia A. Hollander, Esq.

The Higher Education Administration Series

COLLEGE ADMINISTRATION PUBLICATIONS, INC.

COMPUTERS IN EDUCATION: LEGAL LIABILITIES AND ETHICAL ISSUES CONCERNING THEIR USE AND MISUSE

This monograph is a part of
The Higher Education Administration Series
which also includes:

- ☐ Administering College and University Housing: A Legal Perspective
- ☐ The Dismissal of Students with Mental Disorders: Legal Issues, Policy Considerations, and Alternative Responses
- ☐ A Practical Guide to Legal Issues Affecting College Teachers

Other Computer-Related Publications by the Author

Hollander, P.A., Young, D.P. and Gehring, D.D. (Eds.) (1983-) *The Computer Law Monitor.* Quarterly newsletter briefing of computer-related higher court decisions, plus checklists on relevant topics. Asheville, N.C. 28815-0267 (P.O. Box 9267): Research Publications, Inc.

Hollander, P.A. (1984) An introduction to legal and ethical issues relating to computers in higher education. *Journal of College and University Law,* Fall, *11,* 2, 215-232.

Hollander, P.A. (1983) University computing facilities: Some ethical dilemmas. In Baca, M.C. and Stein, R.H. (Eds.), *Ethical Principles, Problems, and Practices in Higher Education.* Springfield, Ill.: C.C. Thomas, Publishers.

COMPUTERS IN EDUCATION: LEGAL LIABILITIES AND ETHICAL ISSUES CONCERNING THEIR USE AND MISUSE

By Patricia A. Hollander, Esq.

The Higher Education Administration Series
Edited by Donald D. Gehring and D. Parker Young

COLLEGE ADMINISTRATION PUBLICATIONS, INC.

College Administration Publications, Inc.,
P. O. Box 8492, Asheville, N. C. 28814

© 1986 College Administration Publications, Inc.,
All rights reserved. Published 1986
Printed in the United States of America
91 90 89 88 87 86 5 4 3 2 1

Library of Congress Cataloging in Publication Data

Hollander, Patricia A.
Computers in education.

(The higher education administration series)
Includes bibliographical references.
1. Education law and legislation—United States.
2. Computers—Law and legislation—United States.
3. Liability (Law)—United States. 4. Education—
United States—Data processing. I. Title. II. Series.
KF4124.5.H65 1986 370'.28'54 86-2610
ISBN 0-912557-03-6

Brief quotation may be used in critical articles or reviews. For any other reproduction of the book, however, including electronic, mechanical, photocopying, recording or other means, written permission must be obtained from the publisher.

The views expressed in this book are those of the individual authors and are not necessarily those of College Administration Publications, Inc.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

—from a Declaration of Principles jointly adopted by a committee of the American Bar Association and a committee of publishers.

Table of Contents

Foreword • *xi*

About the Author • *xiii*

I. **Roles of Law and Ethics Regarding Computers in Education** • 1

- Increasing Use of Computers in Administration, Teaching, and Research • 1
  - Two Tasks for Educators • 1
  - Emergence of "Computer Law" • 1
  - Implications of New "Computer Law" for Academic Traditions • 2
- Typical Legal Liabilities and Ethical Issues Regarding Computers • 2
  - Typical Legal Liabilities • 2
  - Typical Legal/Ethical Issues • 3
  - Three Categories of Legal and Ethical Issues • 3
    - *Copyright / Patent / Trademark / Trade Secret / Contract / Negligence / Crime / Legal-Ethical*
  - Institutional Liability — Individual Liability • 4
- Major Areas of Legal Risks • 4
    - *Acquisition Process / Use of Computers; Making Copies of Software / Commercial Exploitation of Software and Hardware Created by Employees and Students / Faculty and Staff Concerns / Student Concerns / Negligence / Security / Crime*
- Major Legal/Ethical Issues • 4
- Practical Guide • 5
- Recommendations • 5

II. Liability Related to the Acquisition of Computers • 7
- Pre-Acquisition Planning • 7
  - Who Can Help Answer the Number One Question? • 8
  - How Many Computer Systems • 9
  - Separate Systems • 9
- Selecting A Computer • 9
  - Show Me! • 9
  - Compatibility (Or Beware of Gifts) • 10
  - General Rule—Pick Software First, Then Hardware • 10
- Negotiating Contract Terms • 11
  - Typical Acquisition Contract Terms • 11
- Warranties • 13
- Warranty of Fitness For A Particular Purpose • 13
  - Warranty of Merchantability • 14
  - Implied Warranty Compared to Express Warranty • 14
- Remedies for Poor Performance • 14
  - Breach of Contract • 14
  - Money Damages • 14
  - Misrepresentation • 15
  - State Statutes—Deceptive or Unfair Trade Practices • 15
- Recommendations • 15

III. Liability Regarding Copying and Use of Computer Programs • 17
- Making Copies of Software Programs • 17
  - Back-up and Archival Copies • 17
  - "Shrink-Wrap" Licenses and the License vs. Sale Controversy • 18
    - Avoiding the Sale vs. License Controversy • 18
  - Copies for Friends and Co-workers • 18
  - Copying Your Office Program for Use at Home • 19
  - Copy Bought for One Department Duplicated for Use by Another Department, Site Licenses • 19
- Adaptations of Computer Programs • 19
- "Fair Use" of Computer Programs • 20
  - Fair Use Defined • 20
  - Four Factors Determine Fair Use, Site Licenses • 20

    - What is NOT Fair Use • 21
    - Questions About Fair Use of Owned Copies • 21
    - Fair Use of Copies Acquired by License • 22
- "Public Domain" Computer Programs • 22
- Penalties for Copyright Infringement • 22
    - Registration Necessary to Sue • 22
- Copying Deemed Plagiarism • 22
- Making Lawful Copies of Software Programs • 23
- Sales at Discount by Schools or Colleges • 23
- Recommendations • 24

IV. **Liability Regarding Creation of New Computer Software or Hardware by Employees or Students** • 25

- Commercial Exploitation of Computer Software and Hardware Created by Employees and Students • 25
    - Pricing of Products • 26
    - Revenue Sharing • 26
    - Non-School Marketing • 26
    - Ownership • 26
    - Confidentiality Agreements • 27
- Legal Protection of Computer Software by Copyright • 27
- Translations of Computer Programs from One Computer Language to Another • 27
- Derivative Works • 28
- Copyright and Patent Protects Expression or Execution of Idea, Not Idea Itself • 28
    - Examples of Copyrightable Software • 29
- Rights of Copyright Owner • 30
    - Joint Owners of a Copyright • 30
- Registration of a Copyright • 30
    - Why Officially Register a Computer Program? • 30
    - How to Register • 30
    - Giving Others Notice of Your Copyright • 31
    - Effect of U.S. Copyright in Foreign Countries • 32
    - When Does Copyright Protection Begin? • 32
    - Length of Time of Copyright Protection • 32
    - Where to Place Copyright Notice on a Computer Program • 32

- Legal Protection of
  - Computer Products by Trade Secret Law • 33
  - Computer Products by Trademark • 33
  - Computer Programs by Patent • 33
  - Computer Hardware by Patent • 34
  - Mask Works • 34
- Recommendations • 34

V. **Liability Related to Employment** • 35

- Copyrights: Ownership of Software Written by Employees • 35
  - Example—Software Written by Faculty Member • 36
  - General Rule • 37
  - Example—Software Written by Non-Academic Employee • 37
  - Software Created Pre-Employment • 38
  - Lecture Notes During Employment • 38
  - Working Papers and Drafts • 38
  - "Works Made For Hire"—Term of Copyright Protection • 38
  - Transfer of Employee's Copyright to Employer • 38
- Nondisclosure Agreement Between Employer and Employee • 39
- Restrictive Employment Covenants • 39
  - Employees Serving "At Will" • 40
- Personal Use of Employer's Computer • 40
- Computer Software Written by Consultant or Contractor: Specially Commissioned Works • 41
- Ownership of Computer Hardware Invented by Employees • 42
  - Patenting Computer Hardware • 42
  - Ownership of Inventions, such as Computer Hardware • 42
- Recommendations • 42

VI. **Liability Related to Students** • 43

- Students Who Create Computer Programs • 43
  - General Rule • 43
  - Student as Employee of Institution • 43
  - Student Software as Class Assignment • 43

        - Institutional Control Over Student's Creation of Software • 44
        - Student Software Created In Spare Time • 45
    - Recommendations • 45

VII. **Liability for Negligence** • 47
    - Incorrect Computerized Records • 47
    - Improperly Programmed Computer • 48
    - Electronic Bulletin Boards • 48
    - Health and Safety Hazards • 49
        - Video Display Terminals • 49
        - Shock Hazards • 49
        - Radiation • 50
        - Wrongful Death • 50
    - Recommendations • 51

VIII. **Liability Resulting from Inadequate Computer Security** • 53
    - Privacy and Confidentiality • 53
    - Physical Security • 54
        - Controlling Access to Computer, Room or Building • 55
        - Controlling Access to Software • 56
    - Recommendations • 57

IX. **Computer Crime** • 59
    - Federal Computer Crime Statutes • 59
    - State Computer Crime Statutes • 59
        - Examples • 59
    - Unauthorized Use of Computers • 60
    - Interstate Transportation of Stolen Property • 61
    - Recommendations • 61

X. **Insurance** • 63
    - Property Insurance • 63
    - Personal Liability Insurance • 64
    - Home Computer Insurance • 64
    - Recommendations • 64

XI. **Legal/Ethical Issues** • 65
    - Abuse of Students and Other Vulnerable Persons • 65

Abuse of Computers by Students • 65
Institution's Responsibility to Protect Data, Records and Research Stored in Computers • 67
Access to Computers • 67
Faculty Employment and the Development of Computer Programs • 68
Ethical Responsibilities at the Institutional/Departmental/Faculty Level • 69
Unknown Physical Dangers • 70
Recommendations • 70

Appendix I

Computer Law Glossary • 71
Computer Terms • 71
Legal Terms • 73

Appendix II

Checklists • 77
Copyright, Patent, Trade Secret, & Trademark: Some Basic Elements • 78
Acquisition Contracts for Computer Systems • 80
Service Bureau Contracts • 82
Making Copies of Computer Programs—The Legal Perils • 84
"Fair Use" of Computer Programs by Teachers, Scholars, and Researchers • 86
Licensing Computer Software • 88
Employment Contracts re Intellectual Property Rights • 90
Computer Crime Statutes • 92
Insurance for Computers • 98

Appendix III

Copyright Law Amendment Regarding Computer Programs • 100
Public Law 96-517, December 12, 1980 • 100

Appendix IV

Resources for Legal Information in Secondary and Higher Education • 103

Foreword

The use of computers in educational institutions is expanding at a rapid rate. As was true of slide rules in the past, many colleges and universities now require all incoming students to have a microcomputer. Even elementary and secondary schools are introducing computer literacy programs. Both of these factors demand that school administrators and faculties become aware of the legal and ethical parameters regarding computers.

The law in this field has not caught up with the technical advances. This monograph is designed to bring educators up to date with current legal and ethical issues relating to the computer. These issues involve every aspect of computer acquisition and use.

Knowledge in this area is absolutely imperative for educators, not only to protect themselves from legal liabilities, but also to protect their interest in computer programs and other software which they might create.

For those new to this field, this monograph includes an excellent glossary containing both legal and computer terminology. Checklists are also provided for those charged with making administrative decisions.

DDG
DPY
March, 1986

About the Author

PATRICIA A. HOLLANDER is an attorney in Buffalo, New York. Since 1972 she has been the General Counsel of the American Association of University Administrators, and has consulted extensively in the fields of education and computer law. She also speaks before many educational, computer and legal groups.

Ms. Hollander received her J.D. law degree from St. Louis University and did graduate work at Harvard Law School. At the State University of New York at Buffalo, she served for almost a decade as both an administrator and a faculty member in the School of Management and in the School of Law. In spring 1980, she taught at the University of Virginia's Center for the Study of Higher Education, as Visiting Professor.

Ms. Hollander is the author of *Legal Handbook for Educators,* published in 1978. She is co-author with John Pine of *The Public Administrator and the Courts,* published in 1985. She is also co-author of *A Practical Guide to Legal Issues Affecting College Teachers,* with D. Parker Young and Donald D. Gehring, published in 1985. Since its inception in 1983, she has been an editor of *The Computer Law Monitor,* a quarterly publication that summarizes in lay language significant court cases concerning computer technology.

Among her recent writings is the chapter, "University Computing Facilities: Some Ethical Dilemmas," she contributed to Baca and Stein's 1983 book, *Ethical Principles, Problems, and Practices in Higher Education.* Her article, "An Introduction to Legal and Ethical Issues Relating to Computers in Higher Education," appeared in the fall 1984 issue of the *Journal of College and University Law.* Also in 1984, her chapter, "The Chief Student Affairs Officer as Employer and Manager: A Special Risk," appeared in Owens' June 1984 book, *Risk Management and The Student Affairs Professional,* in the NASPA Monograph Series.

Chapter I

Roles of Law and Ethics Regarding Computers in Education

INCREASING USE OF COMPUTERS IN ADMINISTRATION, TEACHING AND RESEARCH

Educators at schools and colleges today—whether they serve as administrators, faculty, or staff—are faced regularly with new legal liabilities and ethical issues that arise out of the presence of computers in classrooms, offices, libraries, and labs. All levels of education—primary, secondary, and post-secondary—are affected. All educational tasks—administrative, teaching, and research—are involved.

The time is ripe, or overripe, for those with any degree of responsibility for computer-related activities at educational institutions to "learn the ropes and draw the lines."

Two Tasks for Educators

Educators will find they have two principal tasks concerning computer software and hardware.

One task is to manage the acquisition of computer software and hardware.

The other task is to manage the general use of computers once they are installed and, in particular, pay attention to the creation of new software and hardware by employees and students. For just as soon as people begin to become familiar with computers, they see ways of writing new programs and documentation, compiling new databases, or developing new hardware.

Every school and college needs policies to deal with the legal and ethical issues related to computers at their institution.

Emergence of "Computer Law"

The law of computers is, for the most part, the law of copyrights, patents, trademarks, and trade secrets. Computers fall into a category of property called intellectual property.

Software, that is, computer programs, documentation, and databases, generally is governed by copyright law.

Hardware, the computer machinery itself, such as keyboards, disk drives and video display terminals, usually is governed by patent law.

When information about new computer software or hardware is kept confidential, that information may be protected as a trade secret.

A logo or "mark" identifying a product or service may be protected as a trade mark or service mark.

Of course, there still will be many legal questions to be handled by the more well-established law of contracts or torts or criminal law.

Implications of New "Computer Law" for Academic Traditions

Traditionally in the academic community, copyrights usually were deemed to belong to the writers of the work, while patents generally were shared in some fashion between the inventor or discoverer and the educational institution.

Today, courts are being asked to apply copyright law and patent law to computer-related matters, and there are new interpretations evolving.

In addition, the many unusual features of computers also are having an impact on contract law, tort law, and criminal law. Even tax law requires rethinking in the light of new interpretations of tangible and intangible property.

TYPICAL LEGAL LIABILITIES AND ETHICAL ISSUES REGARDING COMPUTERS

Typical Legal Liabilities

On almost any ordinary day, educators at colleges and schools may be confronted with an array of legal questions concerning computers. They may arrive in the morning to find that the institution's chief executive office is ready to file suit because:

- the new computer acquired to handle graphics in color will do only word processing in black and white;
- the library's computerized circulation data has been destroyed;
- students have cracked an access code and gotten into the payroll files;
- a faculty member is about to file suit, claiming the copyright to the computer program she developed belongs to her personally, not to the institution; or
- a staff member is using unauthorized time on an institutional computer in the evening to conduct his real estate business.

If the right legal steps were taken in advance, the harried educator could respond that:

- the contract with the supplier of the new computer contains a warranty of fitness for a particular purpose so we will demand that the correct computer be supplied;

- we have back-up copies of the library circulation data secured in the safe in the business office;
- we will discipline the student in accordance with our written policy, change the access code more often, and consider setting up two separate, unlinked computer systems for student/classroom use and business use;
- our written policy regarding software created by faculty covers that situation, and in this instance the new program belongs to the faculty member; and
- our written policy regarding employee use of institutional computers for personal business covers that situation, and in this case had the employee requested permission, it would not have been granted, so a reprimand will be issued and placed in his personnel file.

Typical Legal/Ethical Issues

A typical legal/ethical issue might concern a student who cracked the access code; he ranks first in his class, says it was all in fun just to see if he was good enough to do it, did no damage other than breaking the code, and never before has been in trouble. Shall he be prosecuted criminally in addition to being disciplined by the institution?

The institution may have a policy allowing discretion in some instances of forgiving a first, minor transgression before moving to criminal prosecution.

Three Categories of Legal and Ethical Issues

The acquisition and use of computers by educational institutions generate at least three categories of legal and ethical issues.

The first category concerns relatively unique legal intellectual property issues, related to the law of copyrights, patents, trademarks, and trade secrets. Examples are: who owns the copyright on computer programs developed by faculty, staff, or students; and, may one make copies of computer programs? Computer hardware generally raises questions of patent law.

A second category relates to more common legal issues, such as contract issues regarding warranties covering computers, and tort issues regarding the negligent or wrongful use of computers. Criminal laws affecting computers fall into this category as well.

A third category arises from the fact that educational institutions often wish to respond to what may be termed legal/ethical issues in a different fashion than would noneducational organizations. For instance, educational institutions must decide whether every student who "breaks the code" of a computer to gain access to unauthorized time, for whatever reason, should be turned in for possible criminal prosecution as well as suffering campus penalties.

Institutional Liability Compared To Individual Liability

From the standpoint of the institution itself, civil liability may result in penalties such as injunctions and damages.

From the viewpoint of individuals, there may be both civil and criminal liabilities, possibly resulting in penalties including injunctions, damages, fines, and imprisonment. In addition, individuals may be subject to campus discipline, such as suspension, termination, or expulsion.

MAJOR AREAS OF LEGAL RISKS

Educators at schools and colleges will find risks of liability present in areas of computer-related activity such as:

- the process of acquiring computers, including deciding which computer or system to acquire, and negotiating acquisition contracts;
- the use of computer hardware and software at the institution, including setting policy for appropriate use and penalties for misuse of software and hardware, such as making unauthorized copies of computer software;
- faculty, administrator, and staff (employee) concerns, including making policy and rules regarding the ownership of copyrightable and patentable computer products created by employees;
- student matters, including making policy regarding the ownership of copyrightable and patentable products created by students;
- commercial exploitation of copyrighted and patented computer products developed by employees and students;
- negligence, including trying to avoid improperly programmed computers;
- security, including the protection of computer buildings, equipment, data, and files, and related concerns of privacy and confidentiality; and
- crime, including knowing what constitutes criminal activity and what the penalties are.

MAJOR LEGAL/ETHICAL ISSUES

A number of legal/ethical issues have been generated by the presence of computers at schools and colleges. Among them are:

- abuse of students, as where a faculty person, untrained in the use of computers, threatens a computer wise student that he will fail her unless she gets unauthorized computer time for him to do his research;
- abuse of computers by students, as in breaking an access code;
- responsibility to protect data, records, and research stored in computers;

- access to computers, as in providing opportunity for training in computer literacy;
- close questions regarding ownership of software created at the institution;
- competition for favor between computer-heavy and computer-light departments and individuals; and
- unknown physical dangers, such as radiation from video display terminals.

PRACTICAL GUIDE

This book is meant to be a practical guide that highlights basic legal and ethical questions and suggests specific preventive steps to help avoid some of the more obvious legal and ethical pitfalls related to the acquisition and use of computers in education. It gives tips on how to encourage appropriate use of computers and discourage misuse.

The book begins with some cautionary words about legal liabilities concerning the acquisition of computers.

Then, it moves on to legal issues related to the use and possible misuse of those computers in educational institutions. It also discusses a number of legal-ethical issues related to computers that are bound to arise in any educational enterprise.

RECOMMENDATIONS

Responsible educators at schools and colleges will want to take all reasonable measures to try to avoid computer-related risks. For instance:

- Institutional policy and related documents should reflect computer-related issues;
- Orientation and training of personnel and students on computer-related matters is essential;
- Maintenance of computer equipment must be top quality and ongoing; and
- Risk management, including security measures and insurance coverage, regularly must be reviewed and updated.

For further discussion, see:

Hollander, P.A., Young, D.P. and Gehring, D.D. (Eds.) (1983-) *The Computer Law Monitor.* Quarterly newsletter of briefs of court cases, plus checklists on relevant topics. Asheville, N.C. 28815-0267 (P.O. Box 9267): Research Publications, Inc.

Hollander, P.A. (1984) An introduction to legal and ethical issues relating to computers in higher education. *Journal of College and University Law,* Fall, *11,* 2, 215-232.

Chapter II

Liability Related to the Acquisition of Computers

PRE-ACQUISITION PLANNING

Few acquisitions cry out for careful planning to the extent that computer acquisitions do. Choosing one computer or system over another sets patterns for carrying out the institution's tasks and commits substantial sums of money. It can have an affect on the entire institution, from its recruitment development, to curriculum development, to alumni development.

Educators at schools and colleges contemplating the acquisition of a single computer or several complex systems are confronted with the number one question: What do you want the computer to do for you? This is the first and most critical question to be answered. What functions are to be performed by the computer? Is the computer to drill students in math? Is it to collect data and create a database? Is it to provide word processing? Is it to be used in a research lab? Is it to produce payrolls? Will it be used by one person or by many?

From a legal standpoint, one reason this question is so crucial is that it is directly related to the degree of protection available from warranties. For instance, when you are able to set forth in an acquisition contract what functions a computer is to perform, a special kind of warranty may be created. It is called a warranty of fitness for a particular purpose. It says, in effect, that the computer supplier understands what special functions you expect the computer equipment to perform, that you are relying on his or her judgment to recommend appropriate equipment, and that the equipment being supplied will perform those functions. Then, should the computer fail to perform the expected functions—drilling students in mathematics, doing statistical research, handling student registration, or making out staff payroll checks—legal liability generally would rest with the computer supplier. The supplier would be responsible for repairing the computer, replacing the computer, paying damages, or doing a combination of these things.

On the other hand, where an acquisition contract merely states that a specified set of equipment is being ordered, without indicating what functions are to be performed, only the more ordinary warranty of merchantability may be created. A warranty of merchantability merely provides that the equipment will work properly, not that the equipment will perform particular functions such as those just mentioned above.

Ideally, both kinds of warranty ought to be sought. The warranty of merchantability will guarantee that the equipment will work properly. The warranty of fitness for a particular purpose will guarantee that the equipment supplied is the right equipment to perform the particular, expected functions.

Who Can Help Answer the Number One Question?

Get expert help in answering this question. This may be one of those rare occasions when a team or committee approach to solving a problem is both a real necessity and benefit.

Look for several kinds of experts. One set of experts will already be on the payroll or attending the school or college. They are the faculty, staff and students, in other words, the potential users of the computer. If the computer is to assist with teaching, then faculty and students may help define exactly how the computer is to be used in teaching. The computer may be expected to drill students by asking questions and providing correct answers. It may be expected to assist with grammar and composition. If, rather, it is to be used for payroll, then business office staff ought to be consulted.

A second set of experts needed consists of people knowledgeable about computers. You may have some of these people in-house. But, outside experts from computer software and hardware companies may be needed as well. They will have to deal with questions such as the following. What computer programs are available to do the tasks you want done? What kinds of computer equipment will be needed to run the programs? Will one computer keyboard do? Do you need a screen? Do you need a printer, and if so, should it be a letter quality printer or a less expensive and faster dot matrix printer? Will additional electrical outlets or other changes in present electrical equipment be needed? Are any structural modifications to the buildings required?

A third set of experts are the business office and legal people. They can help decide whether equipment should be leased or purchased. They will help negotiate warranties to cover poor performance of equipment. They may write into the acquisition contracts certain provisions for maintenance and updating of the computer as well as training of personnel.

Finally, it is a good idea to get an independent outside expert to look over all plans before the final decision is made. Find someone who has no particular ax to grind but is competent to understand your needs and make suggestions to improve the entire package.

How Many Computers or Systems?

A fairly standard set of computer equipment for a person who is doing word processing or simple accounting probably would consist of a suitable computer program, a computer keyboard, two disk drives, a screen, and a printer. The word processing or accounting program, along with an operating system program, would be inserted into the two disk drives. The operating system program, to run the system, would go into disk drive number one. The so-called applications program, to do the specific task such as word processing or accounting, would go into disk drive number two. The screen would be used to view work in progress. The printer would produce a paper copy of the work.

Can one get by with less? Yes, if all one wants to do, for instance, is drill students on spelling or math. Then, possibly a printer is not needed. The response on the screen of the monitor may be all that is required. No paper copy, sometimes called hard copy, is needed. Or the keyboard may have one disk drive built in, so all that is needed is one extra disk drive for the applications programs.

On the other hand, if more than one person will be using a computer, several computers may be needed. There are a number of ways of doing this. One way is to have a large "host" computer mainframe or microcomputer with many terminals. Another is to have personal computers, completely separate from one another at each desk or in each office. The possible combinations are vast.

Separate Systems

For security reasons as well as for efficiency reasons, it may be better to have two or three completely separate computer systems. One system may do all business activities, such as accounting and word processing. Another system may do only teaching related activities. Another would handle only research activities. Separate access codes and encryption mechanisms would exist for each separate system.

By having separate computer systems, legal liability connected with security of the equipment itself and with the confidentiality of the information contained in the equipment may be limited.

SELECTING A COMPUTER

Show Me!

Before a contract is written to rent or purchase a computer, ask as many questions about the computer software and hardware as you and your team of experts can think of.

Ask to see similar software and hardware actually functioning, wherever possible. Talk to the users of that equipment. Find out what their computer does well, and what their problems are.

Write into your contract as much protection as possible against similar negative events.

For example, if a computer "goes down," how much time is to be allowed for repairs or replacement before penalties are assessed for unreasonable delays? Is there a "standby" computer available somewhere to handle your work while your computer is being repaired or replaced?

Compatibility (Or Beware of Gifts)

All parts of a computer must be compatible, that is, consistent with the requirements of the basic operating system. Otherwise, they will not work. Make clear who is responsible for ordering all parts, so that liability for damages resulting from the ordering of noncompatible parts is placed properly.

A computer software program that does what you want but will not run on your existing computer hardware is hardly a bargain!

Gifts of computer software and hardware from computer manufacturers, wholesalers, and retailers may be tempting at first glance. But, before accepting any gifts, consider carefully who will pay if the gift items are not compatible with your present system. In the case of gift offers of large numbers of computers, think again whether you want to tie up your entire system with one particular brand of computer. Remember this is a gift with a possible long term string attached to it.

Think twice about compatibility of software and hardware. Liability for mistakenly acquiring noncompatible parts can be very costly where the institution is responsible for the action. The costs include time lost and replacement parts.

General Rule—Pick Software First, Then Hardware

The art of creating and developing software is such that finding software to perform the specific tasks desired may be difficult. Do not despair. Keep looking. Then, when you have found what you want, begin looking for various brands of hardware that will run it.

Do not sign a contract for hardware until you have located the software you want. Think of software and hardware as one complete unit, not two separate units, for one will not perform without the other.

If all else fails, and you cannot locate the software you need, there are several possible alternatives to consider. First, existing software may be adapted, customized, or modified to suit your needs. Second, a completely new software program can be developed especially for you. Both of these possibilities require the expertise of experienced computer programmers. You may have such programmers. You may wish to hire a person or firm to do the modifications or development for you.

Whether existing programs are to be adapted or new programs developed, the contracts for these services must be carefully written so as to provide for your testing the modified or new programs before formally accepting them. A fair amount of debugging and preparation of accurate documentation may be required. Payment should be due only after the programs are found to be exactly what you ordered.

NEGOTIATING CONTRACT TERMS

Are you purchasing a single personal computer or an entire computer system capable of multiple and complex operations?

In any event, you will be negotiating a sales contract.

You may be spending a few hundred dollars, a few thousand dollars, or tens of thousands of dollars. You may be dealing with a small, local, retail computer store or a large, distant, wholesale computer dealer.

Whatever the circumstances, there are several general rules to follow:

1. Know what you want the computer to do.
2. Get independent advice as to several brands and kinds of computers to see.
3. Ask to see the computer in operation, doing what you want it to do. Talk to people who are using it.
4. Get all the terms and conditions of the sale in writing to the extent possible.

Typical Acquisition Contract Terms

The terms and conditions of the contract begin with writing into the sales contract what it is we expect the computer to do, whatever components have been recommended by the salesperson.

Next, the software and hardware components themselves must be specified, unit by unit.

Are all components compatible? Are the various peripheral components compatible with the basic computer equipment? Is the telephone equipment compatible with the rest of the equipment?

The contract, also, must set out answers to questions such as the following:

What are the computer's performance expectations regarding; uptime and downtime, the numbers of users it will accommodate, the speed at which it will operate, whether statistics can be generated, whether reports can be produced in chart, table, or graph form.

Must there be special preparation of the site where the computer is to be housed, such as extra electrical power, heavy duty flooring, raised flooring to house cables, etc. Is air conditioning needed to offset the heat generated by the computer? What site preparation will be done by the seller, and what will be done by the buyer?

Are there dates set forth for delivery, installation, testing of equipment? Is partial payment geared to these benchmark dates? What, if any, are the penalties for delay?

Will the equipment be installed completely by the seller, or will special outside technicians be required for some of the installation work?

What about documentation? Will the seller provide complete and accurate descriptive and instructional materials? What happens if additional materials are needed?

Will the seller's personnel be available to answer questions and give instructions? If so, can they be reached day and night, in person and by telephone?

Who will actually operate the computer equipment? Will it be operated by the buyer's personnel, the seller's personnel, or both? Will the seller's personnel train the buyer's personnel? If so, for how long? Who will train other employees hired later?

What about warranties? Have certain express warranties been made part of the contract? Are there other implicit warranties? A seller tends to wish to disclaim warranties. A buyer generally seeks to secure a warranty of fitness for a particular purpose, so that if the particular purpose is not achieved, both actual and consequential damages can be secured from the seller.

Has the seller arranged for the physical security of the computer equipment, as well as for the security of the data stored in the computer? Are there encryption devices? How is access to the computer controlled? Are there access codes, or other security devices? Is care being taken to reduce fire hazards? Who will train users and other personnel about these matters?

Have arrangements been made for the making and storing of backup copies of computer programs? Storage should be in some other physical location, in a fireproof vault or deposit box. (Incidentally, diskettes require a greater degree of protection, regarding moisture and temperature, than normal "fireproof" safes provide.)

How will maintenance of equipment be provided? Will the seller provide maintenance? Will an outside firm do it? Will the buyer undertake maintenance? What exactly does the maintenance contract provide?

What about emergencies? Suppose the computer "crashes" or "goes down" right in the midst of student registration, or during a payroll run? Is there other equipment that the seller will make available to the buyer so that jobs can be completed without substantial loss of time or money?

Suppose in the future certain modifications need to be made in computer programs or equipment. How will these costs be handled by the seller? Are there discounts available?

Suppose your vendor goes bankrupt. What arrangements have been made to retain access to the updated source code, such as placing it in escrow and keeping it updated?

Financial matters to be settled include the following. Are terms clearly stated regarding rental, purchase, leasing, time-sharing and service-bureau arrangements? What discounts may be applicable now and regarding future dealings? What tax issues may impact the financial package? Are penalties set forth regarding both non or partial performance by the seller and non or partial payment by the buyer?

What insurance coverage should there be for damage to, or injury resulting from, the equipment or the personnel who use it? Is there insurance coverage of possible loss of business?

WARRANTIES

There are a number of warranties possible, such as express warranties that set forth exactly what is warranted, and implied warranties, such as an implied warranty of merchantability or an implied warranty of fitness for a particular purpose. Generally, the warranty that turns out to be of greatest help in a large number of cases is an implied warranty of fitness for a particular purpose.

Warranty of Fitness for a Particular Purpose

Suppose you told a software salesperson that you wanted a computer program that would help your students type class themes and papers, and that you were interested especially in a program that could deal with all those footnotes! You bought the program the salesperson recommended, but when you actually tried it, there was no way for the program to handle footnotes. Is there not some kind of a warranty on which you might rely to try to get your money back?

Yes, there is. The warranty is known as an implied warranty of fitness for a particular purpose. That is, it is a warranty that computer software or hardware is suitable for the special purpose of the buyer, which will not be satisfied by mere fitness for general purposes.

An implied warranty of fitness for a particular purpose arises in just such a situation as the one described above. There, a person set forth the specific functions a program was to do, and relied on the expert advice of the salesperson as to which program to select. By recommending a particular program as one that would meet the specific needs stated, the salesperson warranted that the program recommended was fit for the particular purpose set forth.

An implied warranty of fitness for a particular purpose provides much more legal protection than the more ordinary implied warranty of merchantability.

Warranty of Merchantability

An implied warranty of merchantability merely warrants that a computer is reasonably fit for the general purpose for which it was sold. It does not warrant that it will do anything in particular, such as handle footnotes, or operate at a specific speed, or accommodate manuscripts of a particular length. The seller will have met his responsibility if, for instance, a word processing program does word processing. Only if the word processing program fails to do general word processing, could a buyer claim that the implied warranty of merchantability was breached.

Implied Warranty Compared to Express Warranty

The two warranties just discussed are "implied" warranties. There also are "express" warranties.

An express warranty is one that a buyer and seller usually discuss in detail during negotiations for the acquisition of a program or hardware. An express warranty often is written. A seller expresses exactly what the program or equipment is expected to do. Where there is an express warranty, a buyer generally would have unquestioned recourse to legal redress if the program or other equipment fails to meet the terms of the express warranty.

REMEDIES FOR POOR PERFORMANCE

When a computer does not function properly, there are a number of possible remedies available, depending on the facts of each situation. Breach of contract, claims of misrepresentation and fraud, and violation of state deceptive trade practices acts are common legal theories utilized by purchasers of faulty computer equipment.

Breach of Contract

A breach of contract suit may allege that the seller did not provide the specific computer equipment set out in the sales contract. Or, the breach of contract claim could be that the equipment was not delivered on time, or that only part of the equipment was delivered, or that testing was not done, or the documentation was inadequate or that certain components were incompatible.

Money Damages

Two kinds of money damages may be available. One would be actual damages, and the other would be consequential damages.

For instance, a suit involving a breach of warranty regarding the proper functioning of a computer system resulted in actual damages amounting to the difference between the value of the computer system as delivered and the value of the system as warranted. The amount of damages awarded was over $200,000. *Chatlos Systems, Inc* v. *National Cash Register Corp.*[1]

Consequential damages could be, for example, the monies foregone by a buyer due to the loss of business that was foreseeable by a seller if the wrong computer were delivered.

Misrepresentation

In one case, a court found that a seller negligently misrepresented the capability, suitability, reliability, serviceability, and profitability of a computerized typesetting machine, known as the EditWriter 7500. Evidence produced at the trial showed that the EditWriter did not function as represented. "The RAM board was not functional; the keyboard locked up; the viewing screen blanked out or information shown on the screen did not transfer to the photo unit; the photo unit produced crooked lines, bouncy type, spontaneous capitalization, and shadow images. The disk drive alignment malfunctioned, erasing information recorded onto the floppy disks." The appeals court awarded damages of $117,797.55, including the value of data stored in the machine, lost profits, employees' wages, and the purchase price of the machine. *Barnard* v. *Compugraphic Corporation,*[2]

State Statutes—Deceptive or Unfair Trade Practices

The following situation is a classic illustration of a violation of a state statute prohibiting deceptive or unfair trade practices. Evidence showed that a seller intentionally made fraudulent representations about the state of development of its applications software products in order to induce a buyer to enter into a distributorship contract. The court found that the seller "willfully or knowingly" violated the Massachusetts unfair trade practices act. The award to the buyer was over $4 million. *Computer Systems Engineering, Inc.* v. *Quantel Corp.*[3]

RECOMMENDATIONS

Provide adequate time and support for pre-acquisition planning.

Decide what you want your computer to do.

Ask to see computers in operation like the one you want.

Talk to users of computers like the one you want about their experience.

Do your best to see that the written acquisition contract for your computer contains all the terms and conditions of concern to you.

---

[1] Chatlos Systems, Inc v. National Cash Register Corp. 670 F. 2d 1304, U.S. Court of Appeals for Third Circuit, 1982.

[2] Barnard v. Compugraphic Corporation, 667 P. 2d 117, Court of Appeals of the State of Washington, 1983.

[3] Computer Systems Engineering, Inc. v. Quantel Corp. 571 F. Supp. 1365 and 1379, U.S. District Court for the District of Massachusetts, 1983.

Pay special attention to contract provisions concerning testing of equipment, payment over time as testing benchmarks are passed, updating of equipment (especially software), maintenance, training of users, warranties, and provisions for standby equipment.

Chapter III

Liability Regarding Copying and Use of Computer Programs

Educators at schools and colleges will recognize the need for the development of policies and regulations for classroom and general use of the institution's computers.

In addition to the usual concerns, computers raise the unique legal problem of possible copyright infringement when copies are made of computer software programs. The relative ease and speed with which even novices can make copies of costly, copyrighted computer software programs causes serious exposure of the institution to potential claims of copyright infringement.

Schools and colleges sometimes sell computer equipment at discount to employees and students. This, too, may present legal problems.

MAKING COPIES OF SOFTWARE PROGRAMS

Inevitably, a question arises about the legality of making copies of computer programs. Here are a few of the most common situations.

Back-Up and Archival Copies

First of all, there is the question of whether backup or archival copies of a software program one has purchased outright are lawful. The answer is yes. When a software program is acquired through an outright purchase, the federal Copyright Act specifically provides that backup copies can be made for archival purposes.

The copyright law states:

> . . . it is not an infringement for the owner of a copy of a computer program to make . . . another copy . . . of that computer program provided: . . . (2) that such new copy . . . is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful. 17 U.S.C. Sec. 117 (1980).

Copyright law would not apply, however, where one is not the owner of a program, but a licensee. One then would be bound by the terms of the license contract secured from the copyright owner.

"Shrink-Wrap" Licenses and the License vs. Sale Contract

Educators purchase many computer programs. Buyers of computer programs may say, "I thought when a person bought a copy of a software program, the person became the owner of that copy. Now I hear that sometimes the buyer becomes a licensee, not an owner. What in the world does that mean?

A license rather than a sale could occur where the software purchased was sealed closed in such a fashion that when a buyer tore open the seal, he or she found inside a paper saying the purchaser had been given a license by the copyright owner to use the copy of the program in certain limited, specified ways. This is known as a "tear open" or "shrink wrap" license. A buyer then would be a licensee, bound by the terms of the license from the copyright owner. Conceivably, a license may not permit backup copies.

There are legal questions still unanswered about whether a buyer, who thinks he is becoming the owner of a copy, instead becomes only a licensee, when, in fact, the buyer does not learn about the license until after he has paid for the program and opened the package.

Louisiana has passed legislation recognizing shrink-wrap licenses.

Avoiding the Sale vs. License Controversy

Is there anything one can do to avoid the controversy about whether a buyer who opens a "shrink-wrap" or "tear open" software program is an owner or a licensee of the copy of the program?

One way to avoid the license question would be to negotiate a true purchase agreement directly with the owner of the copyright. This is easier done if one is buying a large computer system, such that one is in direct communication with the owner of the copyright. It is not usually possible when one walks into a neighborhood computer shop and purchases a program there.

In general, legal experts believe that buyers of "shrink-wrapped" programs may assume they are owners of the program they purchased, on the following grounds. Such purchasers are unaware of the alleged license until after they buy the program and tear open the package. They could not be said to have known or agreed to the license arrangement. Therefore, the license is ineffective. As mentioned elsewhere, however, at least one state, Louisiana, has legislated a shrink-wrap license law, which has yet to be tested in the courts.

Copies for Friends and Co-Workers

Sometimes, the "May I copy?" scenario goes like this. "I bought a terrific word processing program, and now some of my friends and co-workers want me to make copies for them. May I make copies for them and charge them what the program cost me, or at least the cost of making a copy? If I may not charge for the copy, may I give it to them free?"

The answer is ABSOLUTELY NOT! Remember that the owner of the copyright of the program has placed the copyright on the program in order to protect it from use without appropriate permission or payment. The copyright owner wants the computer program used by many, many people. But, the copyright owner wants to be paid for that use. Or, at least be asked for permission to use the program. Each time you make an unauthorized copy, whether you sell that copy or give it away, you are depriving the copyright owner of payment for use of the program. You are infringing the copyright owner's exclusive right to earn money through the sale of the copyrighted program.

However, merely lending one's own copy to others does not appear to be an infringement.

Keep in mind that you might be a copyright owner someday!

Copying Your Office Program to Use at Home

The same negative answer goes for a query about whether one can make a copy of a computer program bought for use at the office in order to use it at home.

It is an infringement of copyright to make a copy of an office program for use at home. However, one could get permission from one's employer to borrow the office copy, take it home and use it there, then return it to the office.

Copy Bought for One Department Duplicated for Use by Another Department

A computer program bought by one department cannot be copied for use by another department. Where a single program will be useful to many departments, either buy enough copies for all departments, or consider negotiating a site license that will cover multiple copies at less cost.

ADAPTATIONS OF COMPUTER PROGRAMS

The Copyright Law permits the owner of a copy of a computer program to make an adaptation in order for the program to be used in conjunction with a particular set of computer equipment.

However, an adaptation may be transferred only with the authorization of the copyright owner. 17 U.S.C. Sec. 117.

An adaptation is not considered to be a new work. The individual who makes the adaptation is not considered to be the owner of it.

FAIR USE OF COMPUTER PROGRAMS

Computer programs are protected by copyright as a form of "literary work." Thus, in attempting to sort out questions of fair use of computer programs, it may be helpful to think of a computer program as though it were a book. Generally a copyrighted book cannot be copied without permission of the copyright owner. Similarly, a copyrighted computer program generally cannot be copied without the permission of the copyright owner.

Fair Use Defined

Fair use is a statutorily created (Sec. 107 of the 1976 Copyright Act), permissible use of copyrighted works under certain limited circumstances notwithstanding the rights of the copyright owner.

Fair use of a copyrighted work includes:

> reproduction in copies . . . for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research . . . .

Fair use is not an infringement of copyright.

Four Factors Determine Fair Use

In determining whether a particular use of copyrighted work, such as a computer program or a book, is a fair use, consider:

1. the purpose and character of the use, including whether of a commercial or nonprofit educational purpose;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use on the potential market for or value of the copyrighted work.

Regarding the first of the above factors, the purpose and character of the use, while the doctrine of fair use applies generally to educational settings, the mere fact that copies of a textbook or a computer program are made for a nonprofit educational purpose will not provide an automatic "fair use" defense against a charge of infringement. Textbooks and computer programs are meant for sale to the educational market. The way for an educational institution to get more copies is to buy them, not duplicate them. Bulk purchases of software or negotiation of a site license permitting use of a program throughout a designated site, such as a whole building, campus, or system, are other avenues to pursue.

As to the second factor, the nature of the copyrighted work, most computer programs may be likened to technical writings like operator's manuals. These usually are deemed to be informational rather than creative writings, so fair use could be available as a defense, other facts permitting.

Concerning the third factor, the amount and substantiality of the portion used, the tests applied here involve both quantity—how much was copied—and the importance to the work of that which was copied. As to quantity, excerpts usually are acceptable fair use. Congress contemplated "reproduction by a teacher or student of a small part of a work to illustrate a lesson."[1] Thus, in the case of books, an excerpt could illustrate grammar and the author's style. In the case of computer programs, an excerpt could illustrate programming techniques and show what is source code as compared to object code.

What Is NOT Fair Use

Few would say that copying a whole book for use by students was a fair use. Yet, some try to maintain that copying an entire computer program for use by students is a fair use. Both these copying practices clearly are copyright infringements in all but extraordinary circumstances.

Questions About Fair Use of Owned Copies

Q. May we purchase one copy of a computer program and use it to make twenty other copies for use by students?

A. No, Section 107 of the Copyright Act prohibits reproduction of computer programs in copies and distribution of copies to the public without permission.

Q. May we purchase one copy of a computer program and transfer it from floppy disk to hard disk for use with our hardware?

A. Yes, Section 117 of the 1980 amendments authorizes adaptation as an essential step in the utilization of the computer program with a machine.

Q. May we make a back-up copy of a purchased program?

A. Yes, Section 117 also authorizes a back-up copy.

Q. May we lend our copy of a purchased program to students in serial fashion?

A. Yes, just as you would lend a library copy of a book to students in serial fashion. However, it is not permissible to permit all students to have copies of the program simultaneously, just as it would not be permissible to make enough copies of a book so that all students could have copies simultaneously.

Q. If we purchase twenty copies of a program for use by students in one class, may we use the same twenty copies for a subsequent class?

A. Yes, you may own multiple copies of a computer program and lend them, just as you would lend textbooks. Also, remember to make back-up copies of any programs lent out in case they are destroyed.

---

[1] U.S. Congress, House Judiciary Committee, 90th Cong., 1st Sess., 1967, H.R. Rep. No. 90-83 ("1967 House Report") at 65.

Q. Suppose we are sued by a copyright owner who claims we are aiding and abetting students who make personal copies from the copies we lend them?

A. Reasonable precautions in the classroom to attempt to prevent unauthorized copying will be very helpful in countering such a charge.

Q. Is there some way we can acquire multiple copies of software other than buying them piecemeal?

A. Consider trying to negotiate bulk purchases or persuading software companies to donate copies under tax-favored conditions.

Fair Use of Copies Acquired by License

Where copies of software are not owned, but licensed from the owner, the terms of the license control what copies may be made.

Consider negotiating a site license that will cover use of the software throughout the designated site, such as an entire building, campus, or system. Consider also persuading licensors to donate permission to use.[1]

"PUBLIC DOMAIN" COMPUTER PROGRAMS

Computer programs created by individuals supported in their task by public funds, such as government research grants, often are owned by the government. They are said to be in the "public domain," and may be freely copied and used.

PENALTIES FOR COPYRIGHT INFRINGEMENT

Penalties for copyright infringement include the following:

1. Injunctions against further infringing use;
2. Impoundment and destruction of infringing articles;
3. Actual damages and profits attributable to the infringement;
4. Statutory damages;
5. Costs and attorney's fees; and
6. Criminal prosecution (fine and/or imprisonment and seizure of infringing articles).

—17 U.S.C. Secs. 502-509

Registration Necessary to Sue

Registration of a work with the Copyright Office is a prerequisite to filing suit for infringement of a copyright and seeking an award of damages or fees. —17 U.S.C. Sec. 412.

COPYING DEEMED PLAGIARISM

In addition to being unlawful as an infringement of copyright, copying a protected computer program may be deemed plagiarism, just as would copying any other intellectual work.

---

[1] For further discussion of fair use, see: Brooks, D.T. (1985) Fair use of computer software by educators. EDUCOM Bulletin, Summer 1985, Vol. 20, No. 2.

A school or college should state in its policies or rules what penalties are possible as a result of students' or faculty members' or staff members' copying all or part of a protected computer program and attempting to pass it off as their own work.

MAKING LAWFUL COPIES OF SOFTWARE PROGRAMS

Here is what most legal commentators presently believe one may do with the copy of a computer program one owns:

- "copy" it by using it in a computer's memory;
- make one backup or archival copy;
- make adaptations in order to use in a particular machine;
- lend it; and
- sell it; in which case the backup or archival copy must be destroyed.

Educational institutions also are permitted "fair use," such as copying brief excerpts to demonstrate a programming technique.

SALES AT DISCOUNT BY SCHOOLS OR COLLEGES

Computers sometimes are offered for sale at a discount to teachers, students and staff by schools or colleges that have negotiated discount arrangements with computer companies.

These discount sales may be fought by local computer merchants.

In one instance, a state university, the University of Illinois at Urbana-Champaign, closed its computer-discount store after suit was filed by four computer store owners who alleged the university was in violation of a state statute that prohibits it from interfering with private enterprise. The university turned over the discount sales to a local Computerland store.[1]

In another case, the Board of Regents of the University of Wisconsin System had an agreement with Apple to sell computers to students and staff. The prices charged by the university for resale to staff and students often were lower than those charged by Apple to it's local authorized dealer. The local Apple dealer sued both Apple and the university.

On one issue, the U.S. District Court of the Western District of Wisconsin found in favor of Apple in that Apple expressly had reserved to itself in the dealership contract the right to make unlimited resales and direct sales without notice or liability to the dealer.

On another issue, the court found in favor of the state university system by holding that the university system was entitled to Eleventh Amendment immunity from liability as an entity of the state.

However, on a third issue concerning a possible violation of the Robinson-Patman Price Discrimination Act, the court said it could not grant Apple's request for a summary judgment because there remained material factual disputes about whether Apple's defense under the Nonprofit Institutions Act was sufficient. At issue was whether the provision that university resales to staff and students were conditional on no further resale by staff and students provided enough of a limitation on the discount program to permit the program to be deemed to have an educational purpose. These facts would have to be determined at a trial.[1]

---

[1] Chronicle of Higher Education, March 8, 1985, p. 18, col. 2.

RECOMMENDATIONS

Develop and disseminate a written policy regarding the making of copies of computer software.

Before selling computer products at discount to employees and students, have your legal counsel review the proposal.

---

[1] Computronics, Inc. v. Apple Computer, Inc. and the Board of Regents of the University of Wisconsin System, 600 F. Supp. 809, U.S. District Court for the Western District of Wisconsin, 1985.

Chapter IV

Liability Regarding Creation of New Computer Software or Hardware by Employees and Students

Schools and colleges will find it useful to have a stated policy with regard to legal protection and ownership of computer software and hardware created by employees, such as faculty, staff and administrators, and by students.

Early clarification of ownership is especially crucial concerning computer software. Whoever is determined to be the "author" of copyrightable works, e.g. computer programs, documentation, and databases, now has instantaneous automatic copyright protection in those works as soon as they are in fixed, tangible form. Therefore, even before work begins, the parties should know who is the legal author.

For example, regarding employees, is the employee or the employer the author? In the case of students, is the student or the institution the author?

At most educational institutions, the tradition is that copyrights belong to the writer, unless there is a contract or other agreement to the contrary.

As for computer hardware, patent law generally applies. The tradition at educational institutions usually is that patents are taken out in the name of the individual employee-inventors and then assigned to the institution. Revenues may be shared.

Whatever the arrangement is, regarding ownership of intellectual property, it should be fully understood by all parties, including students, and, preferably, should be in writing.

COMMERCIAL EXPLOITATION OF COMPUTER SOFTWARE AND HARDWARE CREATED BY EMPLOYEES AND STUDENTS

Schools and colleges should have a stated policy concerning possible commercial exploitation of computer products created by employees and students. Where support services for commercial exploitation are available, they should be described.

Where educational institutions choose to market software, for example, the financial return may be substantial. Stanford University expects to earn some $600,000 this year by licensing software written by Stanford faculty members, staff members and students. Stanford has had a software licensing service for commercial exploitation of Stanford-created software products since 1982. Engineering and computer science produce most of the software, ranging from a program that collects data for biology experiments to "Mozart," a program that projects attendance at musical performances.[1]

Pricing of Computer Products

Any school or college contemplating the marketing of software or hardware must make several threshold decisions; for instance, whether to have different pricing policies for software sold to commercial companies as compared to those sold to educational and governmental agencies. Stanford's policy requires commercial companies to pay from $500 to $10,000 to use the programs, while universities and government agencies pay only the distribution costs, which are said to be about $200 for programs for mini- and main-frame computers.

Stanford also has a number of licensing agreements that allow commercial publishers to market computer programs that the publishers have brought up to commercial standards through additional testing and by writing user manuals.

Revenue Sharing

A school or college also must have a policy regarding how revenue from products it markets will be shared. Stanford, for instance, treats income from software licenses it markets like income from patents: one-third goes to the author of the software, one-third to her school within the university, and one-third to her department.

Non-School Marketing

Stanford reports that not all Stanford-created programs are marketed through the university. Some software writers choose to go directly to commercial publishers and negotiate their own arrangements.

Ownership

To reiterate, each educational institution must clarify its policies concerning ownership of software created by its employees and students. Stanford's policy is that the copyright belongs to the writer unless the software is written under contract or agreement with the university.

---

[1] Chronicle of Higher Education April 10, 1985, p. 28, col. 1.

Confidentiality Agreements

In order to legally protect a new work or a trade secret not protected by copyright or patent, it is useful to ask persons with whom a new work or trade secret is to be discussed to sign a confidentiality agreement or trade secret status reminder letter. This would be appropriate, for example, in discussing a new work or a trade secret with a prospective financial backer.

A confidentiality agreement or trade secret status reminder letter states that the new work or trade secret, such as a computer program, code, documentation, data base or customer list, is considered confidential and/or a trade secret, and is not to be divulged or used by parties who have not received written permission from the owner.

LEGAL PROTECTION OF COMPUTER SOFTWARE BY COPYRIGHT

Most computer software programs are protected by copyright. Some are protected by trade secret. In rare situations, usually where a computer program is part of a larger process or machine, programs may be protected by patent.

In the early days of the development of computer programs, there was a legal question as to whether they were in fact copyrightable. There was never any real question about whether computer hardware was patentable.

The copyrightability of computer programs finally was settled in a case called *Apple Computer Inc.* v. *Franklin Computer Corp.*[1] The court held not only that computer programs were copyrightable, but went on to say that computer programs are copyrightable whether written in source code or object code, whether embodied in floppy disks or silicon chips, and whether they are applications programs or operating system programs.

TRANSLATIONS OF COMPUTER PROGRAMS FROM ONE COMPUTER LANGUAGE TO ANOTHER

Where a computer program written in one language, such as Event Driven Language (EDL), is translated to another computer language, such as BASIC, to run on different computer equipment, the translated program generally is not considered to be a new work. A translated program generally is deemed to be a derivative work. The owner of the copyright in the original work generally would be deemed to be the owner of the copyright in the derivative work.

Thus, the copyright covering a computer program written in one language may be infringed by a substantially similar program written in another language. Studying the source code of a copyrighted computer program and then substantially reproducing its manner of operation in another computer language may lead to charges of copyright infringement.[2]

---

[1] Apple Computer Inc. v. Franklin Computer Corp., 714 F. 2d 1240, U.S. Court of Appeals for the Third Circuit, 1983 (settled Jan. 4, 1984).

DERIVATIVE WORKS

Customizations and enhancements of existing computer programs usually are deemed to be derivative works, not new works. Conversions, too, have been found to be derivative works.

Generally, a derivative work belongs to the owner of the original work.

Even where a modified computer program is two-thirds the work of a second party and appears to be "new," the modified work may belong to the owner of the original work.

There may be situations where a second party could find a way to separate his or her work from the original and claim ownership of that part.

In most instances, however, starting with a program owned by another, with no real break in the connection between the two, leads to a modified work owned by that other.

To use such a modified work, one should have the authorization of the original owner. One could pay for such authorization, get it gratis, or arrange a form of shared ownership.

One of the first cases to find that a conversion of a computer program was a derivative works is *SAS Institute, Inc.* v. *S & H Computer Systems, Inc.*[3] The facts in that case led the court to find that there was no real break in the connection between the original program and the modified program.

COPYRIGHT AND PATENT PROTECT EXPRESSION AND EXECUTION OF IDEA, NOT IDEA ITSELF

When a computer program, documentation, or data base is copyrighted, only the expression of the idea, not the idea itself, is protected.

Therefore, it is entirely possible that someone else may come up with another computer program, documentation, or data base expressing the same idea in a different form of expression, and copyright the new work.

For example, there are any number of copyrighted computer programs that do word processing. The idea of doing word processing is not copyrightable. Particular computer programs embodying different ways to do word processing are copyrightable.

---

[2] Whelan Associates v. Jaslow Dental Laboratory, U.S. District Court for the Eastern District of Pennsylvania, 609 F. Supp. 1307, 1985, and 609 F. Supp. 1325, 1985.

[3] SAS Institute, Inc. v. S & H Computer Systems, Inc., 605 F. Supp. 816, U.S. District Court for the Middle District of Tennessee, 1985.

Similarly, a patent protects the form of execution of an idea, not the idea itself. The idea of inventing computer hardware to display information on a video screen may be executed in different ways, each of which may be patented.

Examples of Copyrightable Software

Here are some examples of computer software and ancillary material that could be protected by copyright:

Operating Systems Software Program—

A basic program that actually causes the computer to operate. It usually is written in "object code," that is, a computer language that is readable only by a machine, rather than in "source code," which is readable by humans;

Applications Systems Software Program—

A program designed to accomplish a particular task, such as, registration of students, payroll, or accounts receivable;

Database—

A compilation of information, such as a list of current faculty, staff, and students, or a bibliography of references to computer crime;

Flow Chart—

A written representation of the steps or logical components used in analyzing a problem, often used by programmers to set forth the sequence of commands in a program;

Listing

Computer-printed representation of a program, showing the input or output data resulting from a command to "print" or "list;"

Documentation—

A manual or other written document prepared for systems analysts and programmers explaining, for instance, how to operate a computer system or program. It usually also contains specifications.

Operations or Service Manual—

A written explanation of how a computer system or program operates, prepared for use by persons expected to operate the system or program or provide maintenance;

Updates—

Improvements made to program code, date, documentation, or manuals to correct errors or improve operation. May refer also to new versions of the software for use with new or different hardware. Sometimes called "patches."

RIGHTS OF COPYRIGHT OWNER

A school or college may be the copyright owner of a computer program. Or, the copyright owner may be a faculty member, a staff member, an administrator, or a student.

The owner of the copyright of a computer program or other work has five exclusive rights. The copyright owner may do, or authorize others to do, the following:

1. reproduce copies of the program or work;
2. prepare derivative works, that is, adapt or modify the program; (Note: A modified program may or may not be a new work. Generally, the original parts of the program belong to the owner of the original parts, and the new modifications belong to the author of the new parts. If the owner of the original parts is also the author of the modifications, there is no problem. But, if the original parts are owned by one person, and a different person is the author of the modifications, ownership of the total modified program needs to be clarified.)
3. distribute copies of the program by sale or other transfer of ownership, or by rental, lease, or lending;
4. perform the program or work, that is, play video games in arcades;
5. display the program or work; that is, exhibit the program or listings at conventions and other meetings.

Joint Owners of a Copyright

Who owns the copyright if there are more than one author?

If there are joint authors, they are co-owners, that is tenants in common.

Each joint owner has the right to use or license the computer program, and then must account to the other joint owners.

REGISTRATION OF A COPYRIGHT

Why Officially Register a Computer Program?

A client may ask an attorney, "If it is true that under the new Copyright Act, computer programs are protected by copyright from the moment of creation, why should I go to the trouble of getting a Certificate of Registration from the U.S. Copyright Office?"

The answer is that you will need the Certificate of Registration should you ever wish to bring a lawsuit alleging that someone is infringing your copyright.

The Certificate of Registration will serve as proof in a lawsuit that you are the owner of the copyright of the computer program at issue, and also will be evidence of the date of your copyright.

How to Register

Is it difficult to get a Certificate of Registration, and how much does it cost?

It is relatively simple to register a claim to a copyright and get a Certificate of Registration. It costs $10.00. If you have little or no experience in registering a copyright, seek advice from an attorney familiar with both computers and copyright.

The steps for registering a copyright claim are:

1. *Obtain Application Form TX—*
   from Information and Publications Section, LM-455 U.S. Copyright Office:
   Library of Congress,
   Washington, D.C. 20559
   (Tel. 202-287-8700)
2. Fill out Form TX—
   Before filling out Form TX, read carefully the Basic Information Instructions that were received with the form.

   Author—Keep in mind that the term "author" refers to the person who wrote the computer program, unless that person wrote the program as part of his or her regular employment duties in which case the employer is the "author."

   Deposit—The term "deposit" refers to an identifying material, such as a copy of part or all of the computer program, which must be sent in with Form TX and deposited with the Copyright Office to show what is being registered. Concern was expressed about revealing to the public complete copies of computer programs. To meet this concern, the Copyright Office has developed special deposit rules for computer programs and documentation. Special rules are in effect, too, regarding the deposit of machine-readable databases.

   If you have never before filled out a Form TX or put together a copy of all or part of a computer program to serve as a deposit, get advice from an attorney or other knowledgeable person.
3. Mail Form TX, along with identifying material, and $10.00 to the Register of Copyrights, U.S. Copyright Office at the above address.
4. When you receive your Certificate of Registration from the U.S. Copyright Office, put it in a safe place.

Giving Others Notice of Your Copyright

Act immediately to give others notice of your copyright when your computer program is in usable or finished form. Do not wait until you have filed Form TX with the U.S. Copyright Office.

Place a copyright notice on your program, as follows:

© 1986 Jane C. Doe.

This provides notice of the copyright, the year the program was first published, and the name of the copyright owner.

Effect of U.S. Copyright in Foreign Countries

The above exact form of notice is absolutely necessary if you wish your program to be protected in many other countries. About sixty countries adhere to the Universal Copyright Convention, which recognizes the above form of copyright notice. Do not substitute any other shape for the circle around the "c" when the copyright notice is printed on paper or other material that is markable in the normal fashion. However, when the copyright notice is to appear on a computer monitor screen and the computer will not produce a "c" in a circle, the custom has been to use (c) or the word "Copyright." Adding "All Rights Reserved" may provide protection in some Latin American countries.

When Does Copyright Protection Begin?

Theoretically, your computer program is copyrighted from the moment of creation, that is, when it is in fixed and tangible form. However, were you to be challenged in court about the date your copyright protection began, your lawyer would rely on the date your notice of copyright appeared on the computer program and the date on your Certificate of Registration from the U.S. Copyright Office.

Length of Time of Copyright Protection

The term of a copyright is the lifetime of the author, plus fifty years.

After the author's death, rights go to the author's heirs or assigns.

If there are two or more authors, the term is the lifetime of the last surviving author, plus fifty years.

Where to Place a Copyright Notice on a Computer Program

Where should a copyright notice be placed on a computer program?

A copyright notice should appear on the printed label on the floppy disk containing the computer program, on the screen when the program first appears, and anywhere else where users will see the notice.

Remember that the purpose of the copyright notice is to inform others that the program is protected by copyright. Therefore, it is incumbent on the copyright owner to place the copyright notice in reasonable places so as to let people know that there is copyright protection on the program. The purpose of the notice is not to prohibit people from using the program, just to inform them that before using the program they should get permission from the copyright owner. This may or may not involve paying for the program. Sometimes a copyright owner permits use without payment. But the copyright owner never chooses to permit use without permission, unless the owner has placed the program in the public domain for use by anyone.

LEGAL PROTECTION OF COMPUTER PRODUCTS AS TRADE SECRET LAW

May one use trade secret law to protect a computer product, such as a computer program one writes?

Yes.

The problem is that a trade secret must be kept secret or it will lose its protection. Therefore, if you are planning to use your program yourself, and you and a very few trusted colleagues are the only ones who know the secret, it is possible to protect the program as a trade secret. Also, a trade secret can be reverse engineered.

If, however, you plan to sell or license the program widely, you may be better off seeking the protection of a copyright.

LEGAL PROTECTION OF COMPUTER PRODUCTS BY TRADEMARK

Trademark law can be useful in protecting marketable computer products.

A recent case involving trademark is informative, even though it deals with a secret process rather than computer products.

A professor developed a secret process for acidophilus milk, which the university protected by the trademark, "Sweet Acidophilus." The professor sought a share of the royalties from the university's licensing of the process. The court noted that the university's patent policy, which provided for sharing of royalties, was not intended to cover trademarks or trade secrets. The professor alleged the university owed him a fiduciary duty to share the royalties.

The basic problem was to sort out the ownership rights in this intellectual property, which then would determine whether the university owed a fiduciary duty to the professor to share the royalties.

The court found that the professor had been employed specifically to develop such a process. Therefore, said the court, the secret process protected by trademark belonged to the university, not the professor. The university owed the professor no fiduciary duty to share the royalties received.[4]

LEGAL PROTECTION OF COMPUTER PROGRAMS BY PATENT

Is a computer program patentable?

Only rarely, such as where the computer program is part of a patentable process.

In 1981, the U.S. Supreme Court held that it is possible to protect computer programs by patent where the computer program is part of a patentable process. The specific case involved a patent for a process for curing rubber that incorporated a programmed computer to regulate heat during the curing process.[5]

---

[4] Speck v. North Carolina Dairy Foundation, 391 S.E. 2d 139 (1984).

However, it must be emphasized that it was the total process for curing rubber that was patentable, not the computer program standing alone.

LEGAL PROTECTION OF COMPUTER HARDWARE BY PATENT

Computer hardware, such as keyboards, display screens, disk drives, and blank chips, may be protected by patent.

An application for a patent normally would be prepared with the assistance of a patent attorney. A prototype usually is required.

Each school or college should have a policy concerning ownership and legal protection of computer hardware invented by employees or students.

LEGAL PROTECTION OF MASK WORKS

A semiconductor product may be thought of as containing three parts. There is the chip or silicon wafer itself (hardware). There is the computer program (software). And there is the stencil, known as a masked work, used to make the chip.

In 1984, the Semiconductor Chip Protection Act[6] was passed to create a new form of protection for masked works. This protection is separate and distinct from copyright law. Registration and deposit are required, and failure to register terminates the protection afforded by the act.

The Semiconductor Chip Protection Act established the first new form of statutory intellectual property in the United States in over 100 years. One of the principal goals of the act is to permit the semiconductor industry to combat chip piracy.

RECOMMENDATIONS

Develop and disseminate policies regarding ownership of computer software and hardware created by faculty, administrators, staff, and students.

Develop and disseminate policies regarding support services for commercial exploitation of computer products, especially any contemplated sharing of royalties and revenues.

Make every reasonable effort to assure that individuals are aware of information about ownership and commercial exploitation of work they create before work is begun.

---

[5] Diamond v. Dieher,[5] 450 U.S. 175 (1981).

[6] Semiconductor Chip Protection Act,[6] 17 U.S.C. Sec. 900.

Chapter V

Liability Related to Employment

As was discussed earlier, one of the principal legal issues faced by educators at schools and colleges concerns legal ownership of computer programs and hardware created by faculty, administrators, and staff members. Contracts of employment often do not deal with the issue of ownership of intellectual property. Therefore, it is becoming essential that each educational institution formulate a policy statement on ownership of computer software and hardware created by faculty, staff, and administrators. In developing policy, a number of factual situations should be kept in mind.

COPYRIGHTS: OWNERSHIP OF SOFTWARE WRITTEN BY EMPLOYEES

Employees often ask, "Do I own the copyright on a computer program I write?" Does it matter whether I write it on the computer at work or on my computer at home?"

There are two schools of thought on the answer to these questions.

Computer programs are defined as literary works. Most schools and colleges appear to be following a trend that treats ownership of copyright of computer programs as they do ownership of other literary works, such as books and articles. Faculty, administrators, and staff who write books and articles usually are considered to be the owners of the copyright to those literary works. Generally, then, the employee would own the copyright on a computer program he or she writes. The exception would be where the employee was hired by the school or college to write computer programs as part of the duties of the job. In that situation, any work-related programs an employee writes would be "work done for hire." Such programs are owned by the employer. In fact, the employer, in such a case, would be considered to be the "author" of the software program, and has the right to copyright it.

An employee may say, "But, I wrote the whole program at home on my own computer and on my own time."

What matters is whether writing the computer program was part of an employee's employment duties.

Suppose an individual was hired as a staff person in admissions. One of her duties was to assist in computerizing the admissions process. It would not matter where or when she wrote software programs for handing admissions. Most likely, creating such admissions programs would be considered part of her job. The admissions programs written by that staff person would belong to her employer, and the employer would have the right to copyright them.

On the other hand, if that same employee received permission to stay after work and use the employer's computer to write non-work-related computer programs, such as for use by the teaching faculty in the English department, or, if she wrote computer programs to handle financial budgeting, she would be in a strong position to assert that those computer programs belonged to her. The individual who wrote them probably would be deemed the author and have the right to copyright them.

The second school of thought on this matter takes the position that under the language of the revised Copyright Act of 1976, scholarly writings, such as that often written by faculty and other employees, now are within the course of employment as anticipated by the statute. Thus, they are "works made for hire" belonging to the employer. Under this reasoning, the institution would own the copyright in all scholarly writings. To overcome this presumption, employees of schools and colleges would be required to negotiate individually and explicitly, as part of their employment agreements, that all their writings belong to them.[1]

Example—Software Written by Faculty Member

Does a computer program written by a faculty member belong to the faculty member or to the institution that employs him or her?

Here is a typical example.

A faculty member is assigned to teach English grammar to students who need remedial training.

The faculty member writes a computer program called "Diagramming Sentences Is Fun and Games," which can be used to drill students in the diagramming of sentences.

A big software company wants to negotiate a license with the faculty member to market the program for use in both high schools and colleges.

---

[1] Simon, T.F. (1982-83) "Faculty writings: Are they 'works made for hire' under the 1976 Copyright Act," Journal of College and University law, 1982-83, Vol. 9, No. 4, pp. 485-513.

The employing educational institution takes the position that the faculty member wrote the software program as part of the regular employment duties, and, therefore, the program belongs to the institution. The faculty member contends that the employment contract speaks only about teaching, not developing computer programs. The faculty member believes the diagramming program belongs to him, or her, not to the institution.

Who is right?

A computer program written by a faculty member probably belongs to the faculty member, unless there is a clear understanding that writing computer programs is a part of the faculty member's job.

General Rule

The general rule is that one who writes a computer program is the author of that program, and owns the copyright. An exception exists where one is an employee hired to write computer programs as part of one's job. Then, the computer program is a "work made for hire," and the employer is considered to be the "author" of the program.

In this situation, the issue is what are the normal duties of one employed as a faculty member? That is, would the writing of computer programs be work normally contemplated to be prepared by an employee within the scope of his or her employment?

In this instance, probably not. Here the writing of computer programs probably would be viewed as would the writing of books or articles, and the copyright would belong to the faculty member.

The situation would be quite different, of course if the employment contract expressly discussed the ownership of computer programs.

Example—Computer Software Written by Non-academic Employee

Does a new computer program written by a non-academic employee, staff or administrator, belong to the employee or to the institution?

Generally, such a new computer program would belong to the staff or administrative employee, unless writing the program was within the scope of employment, or agreed to between the employee and the institution.

Let us suppose that a non-academic staff employee in the computer services center writes a computer program called "Deadbeat," which would be very helpful to the student financial records office in keeping track of delinquent student tuition accounts. In trying to sort out whether "Deadbeat" belongs to the staff employee or the institution, the following issues would need to be addressed. Did the staff employee create "Deadbeat" under the direction and supervision of the employer? Or, did the staff employee simply see the possible need for such a program by education institutions in general, and decide to see what kind of a program she could develop for possible sale to her own employer and to other education institutions?

The controlling factors in determining ownership of the copyrighted work are not necessarily whether or not the staff employee used the employer's time and facilities. What is controlling is whether as part of the employment duties, the employer possessed the right to direct and to supervise the manner in which the work was being performed.

In one case, a court held that the use of a government duplicating machine, government paper, and a government secretary did not make two of Admiral Rickover's speeches "publications of the United States" under the 1909 Copyright Act, Sec. 8.[2]

Software Created Before Employment

Software that relates to one's employment but actually was done prior to the time one began work with the employer belongs to the employee.

Lecture Notes During Employment

Lecture notes belong to the person who wrote them. This is true even if they were written completely on the employer's time, and with the assistance of some of the employer's facilities and personnel.

Working Papers and Drafts

Generally, working papers, false starts, and drafts belong to the employee, absent any express agreement with the employer to the contrary.

"Works Made for Hire"— Term of Copyright Protection

The term, or length of time, of copyright protection of "works made for hire" is the lesser of:

- Seventy-five years from publication

  or
- One Hundred years from creation.

Note: the term, or length of time, of protection for "works made for hire" is not the same as for other works, i.e. the life of the author plus fifty years.

Transfer of Employee's Copyright to Employer

Sometimes an employer would like to acquire the copyright to a computer program owned by an employee. This may be done simply by affecting a formal transfer of the copyright.

---

[2] See 17 U.S.C. Sec 105. Public Affairs Associates, Inc. v. Rickover, 284 F. 2d 262 (D.C. Cir. 1960); vacated per curiam on other grounds, 369 U.S. 111, 82 S.Ct. 580, 7 L.Ed. 2d 604 (1982); on remand, 268 F. Supp. 444, 452 (D.D.D. 1967).

The transfer from the employee to the employer must be in writing.[3]

The transfer must be recorded with the U.S. Copyright Office either:

- Within one month of the execution of the transfer; or
- Before another transfer is recorded, in order to prevent subsequent purchasers of the copyright who have no knowledge of the transfer from employee to employer from having potentially superior rights.

NONDISCLOSURE AGREEMENT BETWEEN EMPLOYER AND EMPLOYEE

An employer who wishes to protect new work or trade secrets not protected by copyright or patent should have employees sign nondisclosure agreements.

A nondisclosure agreement states that the employee agrees not to disclose confidential information or trade secrets belonging to the employer.

A nondisclosure agreement generally gives examples of what the employer considers confidential or a trade secret, such as: computer program listings, source codes, object codes, information about current works or those under development, and customer lists.

Such an agreement also usually provides that upon termination of employment, the employee agrees to turn over notes, records, and documentation used, created or controlled by the employee during employment.

RESTRICTIVE EMPLOYMENT COVENANTS

There may be times when a educational institution may wish to limit an employee, who has special computer skills, from accepting employment with competing institutions.

For instance, a college may have an employee who specializes in developing computer programs that collect and process information about prospective financial benefactors. The college may wish to protect its advantage in having such computer programs should the particular employee leave its employment.

In drawing up a restrictive employment covenant, the employer must take care not to so restrict the individual's future employment as to deprive the former employee of the ability to make a living as a computer programmer.

In essence, a restrictive employment covenant must be reasonable as to:

The type of work restricted;—

---

[3] 17 U.S.C. Sec. 204

The time limit during which the work is restricted; and—

The geographic area in which the work is restricted.[4]

Some states, like California, in effect have outlawed restrictive employment covenants, except in some very narrow areas, for example, where there exists a bona fide "trade secret" or where the sale of a business is involved.

An example of a reasonable restrictive employment covenant in the factual situation mentioned earlier perhaps would be one where the employee's future employment is restricted specifically as a creator of computer programs involving prospective donors to similar colleges, for a one-year period of time, and only at higher education institutions within 100 miles of the employer institution.

Employees Serving "At-Will"

Where employees are serving "at-will," that is, "at the pleasure of the employer," is there ordinarily any form of restrictive employment covenant in effect?

No.

In a case involving at-will employees, a court held that since at-will employees are bound by no restrictive covenants, they may immediately and freely compete with their former employer, including the solicitation of customers.[5]

PERSONAL USE OF EMPLOYER'S COMPUTER

May an employee use an employer's computer for personal business?

An employer may set up policy guidelines to permit an employee to use employer's computer for personal business.

Problems arise when an employer has not informed employees what the policy is regarding personal use of employer's computer.

It is not unusual, for instance, for secretaries who operate word processing computers to "moonlight" by providing secretarial services for faculty, staff, and others, outside their normal working hours. Faculty members may wish to do research or carry on some form of outside business activity, using the institution's computer at odd hours.

An employer should promulgate a clear policy regarding the kind and amount of personal use employees may make of an institution's computer.

An employer may not wish to have certain computer equipment used by employees, especially if that equipment provides potential access to confidential records or data.

---

[4] United States v. Dubilier Condenser Corp., 289 U.S. 178, at 293-294 (1983).

[5] Republic Systems and Programming Inc. v. Computer Assistance, Inc., 322 F. Supp. 619 (D. Conn. 1970), affirmed 440 F. 2d 996 (2nd Cir. 1971).

In one case, an employer did not make clear precisely what kinds of restrictions it placed on an employee's use of the company computer for personal business. An employee used the company computer in connection with his part-time real estate business. The employer discharged him, and maintained he was ineligible for unemployment benefits. A court held that the employee's behavior did not disqualify him for unemployment benefits because the employer's rules were not clear regarding personal use of the company computer.[6]

COMPUTER SOFTWARE WRITTEN BY CONSULTANT OR CONTRACTOR

Schools and colleges often need a new piece of software written for them, and may contract with someone outside the institution to do the work. Does a new computer program written by an independent outsider, such as a consultant or contractor, belong to the outsider or to the institution that hired the outsider?

Generally, the new software belongs to the author, that is, the independent contractor or consultant. If an institution wishes to own the copyright of the new program, it should make sure the contract with the independent contractor or consultant expressly makes that clear, and that the compensation paid for the work reflects the fact that ownership belong to the institution.

Ordinarily, an independent contractor or consultant is not an employee. An independent outsider is hired to provide short-term or one-of-a-kind help in situations where an employer does not want to add another regular employee to the payroll and have to pay Social Security and other benefits. Therefore, the new software program created by an independent outsider would not be a "work made for hire" by an employee within the scope of employment.

An exception to this general rule, where the work would belong to the institution, would be where an independent outsider was hired to produce a "specially commissioned" work. Specially commissioned works would include computer work. Specially commissioned works would include computer sub-routines or programs that are:

- parts of a larger computer program so that they qualify as a "contribution to a collective work."
- "translations," as from one computer language to another, e.g. from COBOL to Fortran.
- enhancements or modifications to an existing computer program, such that they would be considered "supplementary works."
- meant to be merged into a single, integrated package of pre-existing works, and, as such, be a "compilation."
- documentation and considered to be "instructional texts."

---

[6] Giss v. Sumrall, 409 So. 2d 1227 (La. App. 1981).

OWNERSHIP OF COMPUTER HARDWARE INVENTED BY EMPLOYEES

Patenting Computer Hardware

Employers have to deal with legal issues regarding the ownership of new computer hardware invented by employees. An employee policy manual or handbook should state clearly the employer's patent policy.

Ownership of Inventions, Such as Computer Hardware

An employee may ask, "Suppose I invent a new piece of computer hardware. Don't I have the right to patent it?

The general rule is that an employee owns his own inventions and patents, unless he agreed they would belong to his employer.

In the academic world, a tradition exists regarding the patenting of inventions and discoveries of faculty and other employees. It is that employees usually assign rights in their patents to their employing institutions, and the revenue received from the license or sale of the invention is shared between the faculty member and the institution. The formula for sharing may be based on a sliding scale or whatever way is agreed upon by the parties.

Even if an employee did not turn over patent rights to his employer, the theory of "shop rights" may apply. Under the theory of shop rights, an employee may patent the invention, but an employer has a perpetual, royalty-free license to use it.

RECOMMENDATIONS

It is particularly important that employees, such as faculty, administrators, and staff, are given clear information about an employer's position regarding:

- ownership of newly created computer software or hardware;
- support services provided by the employer for commercial exploitation; and—
- possible sharing of royalties and other revenues.

Where an employer has trade secrets, employees should be informed about the need for confidentiality and asked to sign confidentiality agreements.

Where one wishes to discuss with others, one's trade secrets or other confidential information about new software or hardware, consider asking others to sign a non-disclosure agreement prior to the discussion.

Develop rules to govern employees' use of the employer's computer equipment, particularly use for personal business.

Employees, especially those who do programming, should be informed about the possible need for personal liability insurance.

It may be helpful for an employer to provide an office or an institutional representative to whom employees may go with questions.

Chapter VI

Liability Related to Students

STUDENTS WHO CREATE COMPUTER PROGRAMS

General Rule

Educators at schools and colleges may be asked: Does a student own a computer program he or she creates? The answer is: Generally, yes, but not always.

Students' legal relationship with their institution usually is based on their contract of enrollment. There is usually little or nothing in a contract of enrollment that would entitle an institution to ownership of a student's work.

Under the Copyright Act, a computer program is copyrighted automatically as soon as it is in tangible, fixed form. This means that a flow chart, as well as the final form of the program, is copyrighted as soon as it is in tangible, fixed form. Therefore, as soon as a student creates a flow chart or a final program, the work is copyrighted, and the student owns the copyright.

This is so because ordinarily the person who creates a computer program is considered to be the "author" of the program; and the author owns the copyright. Then, a student would own the copyright.

Student as Employee of Institution

There could be conditions under which a student who created a computer program would not be considered the "author." For instance, a student may be hired or commissioned by an institution specifically to develop a computer program for the institution. The program, then, would be a "work made for hire," and the "author" would be the institution. The institution would own the copyright from the moment of creation of the work.

Student Software as Class Assignment

A more troublesome instance would be where a student creates a computer program as one of the assignments for a course, or as a project meeting the academic requirements for a graduate degree.

Educational institutions only recently have begun developing policies to deal with the growing number of situations where students write computer programs which prove to be valuable commercially, such as games or business or educational applications programs.

A situation of this nature between a student and an institution usually is viewed as one involving ethical considerations as well as purely legal considerations. The relationship between a student and an institution generally is rather one-sided, with most of the power residing in the institution. Therefore, care must be taken to treat students in these situations in an authentically fair and open fashion. No institution wants to develop a reputation for using "sharp practices" in its dealing with students.

Institutional Control Over Student's Creation of Software

Where a school or college wishes to claim ownership of student works created to meet academic requirements, the institution should set forth explicitly in the students' contracts of enrollment and in the institution's documents, such as, its admissions materials, its governing board policies, its student handbook, its course descriptions and its degree requirements in its catalogue, or in other similar documents—that in academic matters the institution has the right to give students direction and supervision, through its faculty and staff, such that all work created by students to meet academic requirements belongs to the institution. When such steps have been taken and a computer program is created by a student as part of the academic work required for a course or degree, the institution could take the position that the institution was the true "author" of that program and owned the copyright. The institution might then sell or license the computer program, and share the revenues with the student, perhaps in the form of tuition credit.

The above student/institution situation would be analogous to an employee/institution situation in which a court has held that:

> The essential factor in determining whether an employee created his work of art within the scope of his employment as part of his employment duties is whether the employer possessed the right to direct and to supervise the manner in which the work was being performed.[1]

The **Scherr** court went on to say that:

> Other pertinent, but nonessential, considerations are those indicating at whose insistence, expense, time and facilities the work was created.[2]

---

[1] Scherr v. Universal Match Corp., 417 F. 2d 497, at 500, 164 U.S.P.Q. 225, U.S. Court of Appeals for the Second Circuit, 1969.

[2] Scherr, supra, at 500-501.

Student Software Created in Spare Time

A growing number of students create computer programs in their off-hours, that is, on their own time and not for course credit. A student may or may not use some of the institution's facilities, such as its computer. Again, to call upon an employment analogy, the student probably owns the computer program created. See *Public Affairs Associates, Inc.* v. *Rickover,*[1] where the court held that use of a government duplicating machine, government paper and a government secretary did not make two of Admiral Rickover's speeches "publications of the United States" under the 1909 Copyright Act[2].

The above situation has been dealt with by some institutions by asking students to compensate the institution for the cost of the use of institutional equipment, such as a computer. However, this poses problems since students may have paid tuition for general use of institutional equipment. Also, it is not at all uncommon for such institutional equipment as athletic, theater, art, and laboratory equipment to be used freely by students in off hours.

RECOMMENDATIONS

Develop and disseminate policies regarding ownership of computer software or hardware created by students.

Inform students about any possible support services for commercial exploitation.

Make clear to students whether any sharing of royalties or other revenues is expected.

Help students understand the need for legal protection of their work, including their asking others to sign confidentiality agreements before revealing their work to others.

Help students understand the possible need for programmers to have personal liability insurance.

Provide an office or individual to answer students' questions.

---

[1] Public Affairs Associates, Inc. v. Rickover, 284 F. 2d 262 (D.C. Cir. 1960); vacated per curiam on other grounds, 369 U.S. 111, 82 S.Ct. 580, 7 L.Ed. 2d 604 (1962); on remand, 268 F. Supp. 444, 452 (D. D.C. 1967)

[2] 1909 Copyright Act, Sec. 8. See 17 U.S.C. Sec. 105.

Chapter VII

Liability for Negligence

INCORRECT COMPUTERIZED RECORDS

Most schools and colleges have offices that perform various record keeping functions where there is a potential for error, such as student admissions and records, personnel, and business services.

Is an institution liable for damage or injury caused by incorrect computerized records?

Very likely.

It is becoming increasingly clear that a school or college that relies on incorrect computerized records and thereby causes an injury may find that it is liable under tort theory.

Because records that are computerized tend to be intimidating, some staff members appear to be reluctant to listen to or act upon proffered correct information.

Take the instance of student financial records at post-secondary institutions. A student may be threatened with expulsion or suspension due to an alleged delinquent tuition payment. The student may bring in a cancelled check to show that the computerized record probably is incorrect. The staff in the financial records office may be reluctant to act, mainly because there is no clear and simple mechanism available to allow corrections easily of the computerized records. Were a student to be able to show damages resulting from this set of facts, tort liability may accrue to the institution.

Something similar could occur regarding the forwarding of an incorrect academic transcript, or an incorrect personnel record.

An example of such a tort claim arose in a non-academic setting. An auto credit company relied upon incorrect computerized records with regard to payments for the purchase of a car. The car purchaser offered correct information to the company, but the company persisted in its error and repossessed the car. A Missouri court ordered both actual and punitive damages.[1]

In a case decided by the Supreme Court in 1985, a credit reporting agency sent five subscribers a false report that a contractor had filed a voluntary petition for bankruptcy. The contractor sued the credit agency, alleging libel. The contractor sought presumed and punitive damages. The Supreme Court was asked to rule on the issue of whether the contractor had to prove that the credit agency acted with "actual malice." The Supreme Court held that the contractor did not have to show "actual malice" in order to recover.[2]

IMPROPERLY PROGRAMMED COMPUTER

An improperly programmed computer could cause damages for which an institution may be held liable.

Computers often are blamed for the mistakes of the human beings who program or operate them. Granted, there are occasions when a computer itself makes an error, usually due to an electrical surge or similar glitch. More common is a situation where the person doing the programming, or the person responsible for seeing that the programming was done correctly, simply was not careful enough.

Let us imagine that a student handbook provides that where a student is drunk in class, he is subject to possible suspension or expulsion after a due process hearing. Let us further suppose that the handling of student disciplinary cases have been "computerized." However, the computer programmer forgot to program the computer to send out appropriate due process information concerning notice of the charge and opportunity for a hearing prior to declaring the student suspended or expelled. The institution may be liable for deprivation of due process, and may not be permitted to rely on the excuse that its computer was not properly programmed.

In a case involving a public gas utility, an appellate court found that the due process termination notice, given to the utility's customers prior to their gas being turned off, was inadequate because of an improperly programmed computer. Here, the court held this violated customers' Fourteenth Amendment due process rights. The court ordered the gas company to follow in the future the court's precise instructions as to the content and timing of service termination notices.[3]

ELECTRONIC BULLETIN BOARDS

Questions of possible legal liability surround the use of computer bulletin boards, a high-tech version of the supermarket bulletin board where people advertise services and goods for sale and pass along other messages. For example, would a school or college be liable for negligence if bulletin boards located on their computers contained information that harmed others? Or, if criminal activity were involved, would they be guilty of aiding and abetting?

---

[1] Price v. *Ford Motor Credit Co.*, 530 S.W. 2d 249, Missouri Court of Appeals, 1975.

[2] Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., No. 83-18, U.S. Supreme Court, June 16, 1985, 53 U.S.L.W. 4866.

[3] Palmer v. Columbia Gas of Ohio, Inc., 479 F. 2d 153 (1973).

Electronic bulletin boards are set up by computer users, generally to exchange, via computer, information about new programs, documentation, databases and other matters of special interest to users.

Legal problems arise when, among other information, there appear on electronic bulletin boards items such as: telephone credit card numbers; methods of breaking into corporate, hospital, or government computers; copyrighted software programs; and bank account numbers.

In 1984 an individual was charged with a misdemeanor when his home computer bulletin board was found to contain telephone credit card numbers obtained without authorization. Police seized his personal computer and data storage devices. He was accused of knowingly and willfully publishing telephone credit card numbers with intent they be used to avoid the charges. His defense was that the numbers were published by someone else and that he did not knowingly publish them. The case still is not concluded.[1]

Electronic bulletin boards are being monitored now by telephone companies, government authorities, and software companies, among others.

Schools and colleges would be well advised to attempt to monitor regularly, bulletin boards at their institutions. Enlisting the services of student computer "hackers" to assist in the monitoring could be very helpful.

Illegal, obscene or abusive messages should be removed. When misbehaving individuals are located, appropriate penalties should be assessed.

HEALTH AND SAFETY HAZARDS

Video Display Terminals

Eye problems are reported by persons who work before video display terminals (VDTs). Complaints include: headaches, blurring of vision, itching and burning eyes, eye fatigue, flickering sensations, shooting pains and double vision. The American Optometric Association is instructing its members on how to diagnose and treat the new ills associated with advanced computer technology.[2]

Shock Hazards

Shock hazards sometimes are discovered. One company, Texas Instruments, Inc. reported the remote possibility of a transformer failure resulting in electric shocks to users and damage to the computer regarding their model 99-4A. The company placed large ads in newspapers to warn of the possible danger. This kind of public announcement is both rare and commendable.[1]

---

[1] The New York Times, November 12, 1984, p. 1, col. 1.

[2] Buffalo News, July 7, 1983, p. B-7

Radiation

Radiation emitted from terminals is being studied as a possible danger for pregnant operators. No conclusive results have been published to date, according to recent information.

References

1. *VDT Risks Program,* 9 to 5 National Association of Working Women, 1224 Huron Road, Cleveland, Ohio, 44115.
2. *VDTs In the Workplace: A Study of the Effects on Employment.* 1984. Washington, D.C.: The Bureau of National Affairs, Inc.
3. *Towards a More Humanized Technology: Exploring the Impact of Video Display Terminals on the Health and Working Conditions of Canadian Office Workers.* 1982. Canadian Labour Education and Studies Centre, 2841 Riverside Drive, Suite 301, Ottawa, Ontario, K1V 8N4, Canada.

Wrongful Death

There have been several instances of computer-related wrongful deaths. Two examples follow.

First, in a very unusual case, a court found that the death of a computer systems supervisor was job related so as to sustain an award of death benefits under a worker's compensation law. An employee who worked as a cashier was promoted to office manager and given supervisory responsibility over seven other employees and a computer system. The worker put in long hours both in the office and at home studying the lengthy computer system operations manual. The worker often arrived home from work exhausted, and yet continued to carry office work home. It happened that this individual had a history of systemic lupus erythematosus, an inflammation of the skin and connective tissues throughout the body, dating back several years. Soon the employee was hospitalized, her condition continued to deteriorate, and she died several months later.

The employee's survivors asked for death benefits under the state worker's compensation statute, and the employer appealed. The court found that while the work itself "did not cause the underlying disease, 'it is very probable . . . that the stress, effort, and chronic fatigue incident to her . . . death was an important factor in precipitating an acute exacerbation (and) systemic spread of the condition, (and) hastened, excited and accelerated' the employee's death." The appeals court

---

[1] Buffalo News, February 23, 1983, p.A-6.

A second example involved a worker on an assembly line who was killed by a robotic arm. The legal liability in this case is not yet determined.

These examples point to the need for monitoring of the physical well-being of individuals working with computers as well as the need for monitoring the mechanical maintenance of computer machinery.

RECOMMENDATIONS

Inform employees about legal liability possible as a result of any injury or damages caused by incorrect computerized records, improperly programmed computers, or unauthorized information on electronic bulletin boards.

Take reasonable steps to provide safe and healthful working conditions where computer equipment is involved.

Be especially aware of dangers from fire at computer sites, particularly dangers from toxic fumes.

Chapter 8

Liability Resulting from Inadequate Computer Security

Liability may arise as a result of poor security planning and lack of implementation of appropriate countermeasures to threats to computers.

Computer systems require protection against both attacks and failures. There are a number of security measures that should be considered in protecting computers from either accidental or deliberate threats. When security measures fail, the losses in time and money may be substantial. There may be a loss of availability of the computer, such that service cannot be provided as scheduled or at all. There may be a loss of integrity, such that the computer no longer performs properly. There may be a loss of confidentiality, such that unauthorized persons have access to data. There also may be a loss of data or of monies.

To take care of those situations where security measures do not prevent attacks or failure, there need to be contingency plans to handle whatever eventuates.

Risk management, especially adequate insurance coverage, is essential.

PRIVACY AND CONFIDENTIALITY

Schools and colleges have a special concern to protect the privacy and confidentiality of their records and research data.

It is well recognized that educational institutions are constrained by certain privacy statutes. The federal Family Educational Rights and Privacy Act of 1974 (FERPA), known as the Buckley Amendment, provides for privacy of student academic records by permitting access only by the student and certain authorized persons.[1]

---

[1] Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232g (1976 & Supp. V, 1981).

Educators have asked whether the practice of computerizing record keeping has made it impossible to meet the confidentiality requirements of laws such as the Buckley Amendment.

Computer experts point out that confidentiality of computerized records and data can be maintained in several ways.

Access codes can be used in connection with computerized record keeping, in order to provide confidentiality on the one hand and appropriate access on the other.

Access codes will protect certain "fields of information so that only authorized persons are able to reach certain information. For instance, a record clerk may be given an access code that will permit seeing a person's name, address, and any other information relevant to the clerk's job. But that access code may not enable the clerk to see academic grades, or, perhaps, certain financial information about a particular student or employee.

Research data, likewise can be protected by the use of access codes or by encryption devices.

In addition, some institutions use three separate computer systems, unconnected by telephone or other similar communication, for the institution's business records, its research data, and its teaching materials.

Identifier numbers are another matter often brought to the attention of legal counsel. In general, it is a wise idea not to use social security numbers as identifiers. Under the provisions of statutes such as the federal Privacy Act[1] and the Social Security Act,[2] individuals may have the option of not revealing their social security number. An institution that refuses to recognize such an option may be in violation of the law.[3]

PHYSICAL SECURITY

Liability for negligence in caring for computer equipment and personnel is an issue that requires some discussion. There are foreseeable injuries to computer equipment and personnel that require reasonable preventive measures to be taken.

To mention just a few examples, reasonable steps should be taken to prevent injury and damage due to:

- unauthorized access to a computer site, whether it is a building or a room;
- heat and dust, due to poor air conditioning;
- smoke and fire;
- water, including floods.

---

[1] Privacy Act, 5 U.S.C. Section 552a and note (1982).

[2] Social Security Act, 42 U.S.C. Section 405(c)(2)(C)(i, iii) (1976 & Supp. V, 1981).

[3] Doyle v. Wilson, 529 F. Supp. 1343, U.S. District Court for the District of Delaware, 1982.

The physical security of computers is largely dependent on the locale and design and construction of the building in which the computer is housed.

Where a new building is being built, consideration can be given to a number of important environmental factors, such as whether there are chemical plants nearby emitting harmful fumes, whether the ground is solid, whether electrical storms are frequent, and what the risks are regarding floods, wind, and ice.

Where an old building is being renovated, there may be very little opportunity to avoid such risks.

In either case, building materials used should be of the kind that do not emit dangerous fumes when warm or burning.

Computers placed above ground level can be better protected from flooding. Where computers must be placed below ground level, pumps and similar devices should be provided.

Emergency exit doors should be plainly marked and well known.

Electrical power supply is a paramount importance. There should be a backup power supply in case the main power supply is interrupted.

Electrical power line filtering devices are helpful in avoiding damage that can be done by surges, spikes or "noise" that may occasionally occur in your source of electrical energy.

Air conditioning will probably be a must for most uses of computers. Proper ventilation is required to maintain appropriate humidity and temperature, and dust must be kept to a minimum.

Static electricity can erase data from disks, so floor coverings should be anti-static to whatever degree possible.

Outside, a wall surrounding the building but away from it should help discourage intruders and vandals. This creates a "safety moat" around a building. Obviously, this is an extreme security measure that may be appropriate only in a few instances.

Controlling Access to Computer, Room or Building

First, for any controlled access system to be effective, it must be viewed as valuable by the people involved. Without the cooperation of human beings, almost any access control system can be breached. Therefore, one of the most important steps in setting up a controlled access system is to make clear to people why it is important. Obvious reasons include the physical safety of personnel and equipment from vandals and even terrorists.

Second, the institution must make clear how important it considers the access control system to be, and what penalties and sanctions will be applied for nonadherence to the access rules.

As for methods of restricting access, computer security experts often refer to three basic ways:

- controls using people;

- controls using mechanical locks; and
- controls using electronic systems.

People, such as secretaries and security guards, may be used to screen and challenge persons seeking access to a computer. Authorized persons may be identified by placing their names on a list, or by issuing passes or badges. Whoever is serving as a checker must be trained carefully as to what to do if help is needed.

Mechanical locks using conventional keys may be helpful but are circumvented easily. They are, of course, better than nothing.

Electronic systems often use card keys and key pads, singly or in combination, to control access. These, too, can be circumvented, but not as easily as mechanical locks.

Another form of electronic access control involves wearing a small, electronic transmitter that, in turn, controls locks.

From time to time, security systems need to be changed or updated to decrease the likelihood that persons will become so familiar with the system that they learn to circumvent it easily.

Controlling Access to Software

Liability for damage done to software programs and data stored in computers can be significant.

Passwords and other code words often are used to control access to computer programs.

Both operating system programs and applications programs need to be protected by reasonable means. Damage to or loss of operating system software can shut down completely any use of a computer. Damage to or loss of applications programs can halt whatever particular service depends on the applications programs, such as accounting services, payroll services, registration of students, record keeping of grades, library services, or collection and analysis of research data.

Operating system security measures may be built right into the system by the manufacturer, or they may be added on later. One school of thought is that if the operating system security measures are built right into the system, then any systems programmer may be able to evade them, though other staff members may have a harder time doing so. An add-on security system, on the other hand, may be known only to a very select group of persons so that it is harder to evade by all concerned.

The access control system for software should:

- identify every user;
- maintain access controls over data, programs, processes, and resources, so that only authorized users can access them in authorized ways;

- maintain a log of all use, including alerting staff of attempted breach of the security rules; and
- be secure, so that security checks cannot be evaded, and the log cannot be changed.

A number of companies specialize in developing secure operating systems. They can be costly and cumbersome. The costs and benefits of such security packages must be weighed carefully.

This is a field in which expert advice must be sought.

RECOMMENDATIONS

Carefully select and train employees and other users of computer equipment.

Explain to employees and students the importance of maintaining privacy and confidentiality of certain computerized records.

Review and monitor regularly the security arrangements for computer sites, equipment and data.

Have contingency and recovery plans to handle situations involving breach of computer security or damage to equipment, including backups for software and standbys for hardware.

Chapter IX

Computer Crime

Crimes involving the use of computers can cost schools and colleges substantial sums of money. Institutions should inform faculty, staff, administrators and students what the institution's policy is regarding prosecution of criminal activities. Perpetrators must be prepared to face both external and campus penalties.

Fraud, embezzlement, theft, trespass, invasion of privacy, physical damage to equipment and information, and extortion are among the more standard crimes connected to the use of computers. In addition, two other crimes need to be mentioned as matters of special interest. They are: unauthorized use of computers and the interstate transportation of stolen intellectual property.

FEDERAL COMPUTER CRIME STATUTES

Congress recently passed two federal statutes aimed at criminal acts involving computers. They are the Federal Comprehensive Crime Act of 1984 and the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. These statutes make almost all computer-related fraud, theft, tampering or destruction a federal offense.

STATE COMPUTER CRIME STATUTES

At least nineteen states had computer crime statutes on their books as of September 1984. They are: Alaska, Arizona, California, Colorado, Delaware, Florida, Georgia, Illinois, Michigan, Minnesota, Missouri, Montana, New Mexico, North Carolina, Ohio, Rhode Island, Utah, Virginia, and Wisconsin. Legislation was about to be passed also in Hawaii, Massachusetts, and New York.

Examples

Computer crimes are characterized in present legislation as:

- deceiving a machine;
- computer fraud (with and without intent to deceive);

- altering computerized credit information;
- computer damage or destruction;
- offenses against computer users;
- unauthorized use;
- modification or destruction of programs or data;
- use of computer to commit: embezzlement, fraudulent disposition of personal property, larceny, larceny by conversion;
- tampering or alteration of computer;
- unauthorized access;
- denial of computer services;
- altering or destroying programs;
- computer trespass—removing data, causing malfunction, alter, create, or erase data;
- extortion via threats to damage computer;
- theft of computer-related materials;
- theft of computer services;
- computer invasion of privacy—unauthorized examination of personal or financial data;
- personal trespass by computer, cause physical injury;
- offenses against computer data programs;
- offenses against computer equipment and supplies;

Penalties range from ninety days to twenty years of imprisonment, and from $100 to $150,000+ in fines.

UNAUTHORIZED USE OF COMPUTERS

The unauthorized use of a computer is perhaps the most common computer crime on campus. Typical examples include: (1) a student logging on in order to gain some extra skill in computer use; (2) a faculty member logging on in order to do some non-work-related personal business; and (3) the person who wishes to damage or alter data or other information stored in the computer.

Along with a wide range of unauthorized uses, there are degrees of intent to do mischief. An educational institution must have a policy for how it will respond to varying degrees and types of unauthorized use. Its response may range from a slap on the wrist to the filing of a criminal charge.

Regarding criminal prosecution, it was not a simple matter to prosecute for unauthorized access to a computer in the days when there was no specific language to cover such behavior in a criminal code. An early unsuccessful prosecution in 1977 involved a graduate student's unauthorized use of a university computer in order to complete the research necessary for his doctoral dissertation. In that instance, faculty members responsible for his getting authorized access to the computer apparently failed to make the necessary arrangements. The student simply took matters into his own hands, found a way to learn the proper access code to log on to the computer, and used computer time which he billed to various university accounts. The student was charged with larceny under the Virginia Criminal Code. Ultimately, a court held the unauthorized use of the computer here was not a larceny because of the particular wording of relevant portions of the Virginia Code.[1]

Now, many states have modified their criminal codes in order to make unauthorized use of a computer a crime. So, an institution needs to examine its own state's criminal code before writing its policy regarding how it will respond to unauthorized use of its computer.

INTERSTATE TRANSPORTATION OF STOLEN INTELLECTUAL PROPERTY

An interesting legal question arose as to whether stolen intellectual property, such as copyrighted material, is the kind of property intended to be included in the coverage of the National Stolen Property Act.[2]

This issue appears to be on its way to being settled by the courts. A federal appellate court held that the interstate transportation of stolen intellectual property, which in this case was unauthorized copies of copyrighted motion pictures, is a violation of the National Stolen Property Act.[3]

Schools and colleges should keep in mind, therefore, that federal jurisdiction may be available where a state statute provides inadequate protection to the institution regarding stolen intellectual property.

RECOMMENDATIONS

Make available information about federal and state penalties for violations of computer crime statutes.

Develop and disseminate policies on internal discipline as well as external criminal and civil prosecution for violations of rules and laws.

Follow your own rules and procedures.

---

[1] Lund v. Commonwealth, 232 S.E. 2d 745, Virginia Supreme Court 1977.

[2] National Stolen Property Act. 18 U.S.C. Sections 2311-2319 (1982).

[3] U.S. v. Belmont, 26 BNA's Patent, Trademark & Copyright Journal, 471 (1983).

Chapter X

Insurance

Any plan for risk management relies heavily on insurance.

Schools and colleges will want to ascertain what insurance coverage is available to cover losses due to:

- damage to computers, programs, and data;
- loss of business;
- injury to and by personnel.

PROPERTY INSURANCE

Property insurance is one answer. However, any property insurance policy should be combined with an on-going practice of making back-up copies of everything, and with a system of protection against electrical surges.

One kind of insurance coverage for business computers can be purchased as part of general business insurance. A common example of general business insurance would be an "all risks" policy that covers the insured for all risks except those specifically excluded. Generally, this would cover against accidental damage caused by: fire, water, storm damage, explosion, theft, malfunction of other equipment, vandalism, and perhaps malicious damage.

Another kind of coverage is a special computer insurance policy that specifically may cover computers, terminals, peripherals, programs, data, and storage media. There also is coverage available for computers while in transit from one site to another.

Special attention should be paid to insurance coverage for software programs and data. For example, ask whether the insurance will pay only to replace blank floppy disks, or will pay the cost of reentering the data on the disks. Ask also whether the insurance covers floods, earthquakes, and mechanical and electrical breakdown. Also, does it cover data erasure by magnet or electricity? And what about programming errors?

PERSONAL LIABILITY INSURANCE

Programmers should consider personal liability insurance that covers material loss resulting from errors in a program, or omission of data from a program or database.

HOME COMPUTER INSURANCE

If a computer is used only for home purposes, such as games and hobbies, a homeowner's policy or renter's policy may provide protection. This may involve paying an additional premium to your insurance company for a "floater," "rider," or "endorsement" to your policy to cover the computer.

If, however, a computer is used for work, even at home, it may be defined for insurance purposes as a "business machine" and the insurance company will not pay full replacement value, but only depreciated value.

RECOMMENDATIONS

Review and update present property and personal liability insurance.

Monitor conditions to keep track of possible changes requiring modifications of insurance coverage.

View risk management as including: periodic updating seminars for administrators and supervisors about legal liabilities; competent training of computer users; and proper maintenance of computer equipment and facilities.

Chapter XI

Legal-Ethical Issues

There are certain occasions when a school or college feels obliged to respond to situations in a different manner than other organizations. These times usually are when a particular situation involves a combined legal-ethical matter. More often than not, students are involved. There also are a number of legal-ethical situations regarding faculty, staff and administrators.

ABUSE OF STUDENTS AND OTHER VULNERABLE PERSONS

First of all, how should an institution respond when a student is abused in connection with the use of computers?

Should not an institution come down hard on the perpetrators of abuse of students in such situations?

For example, a faculty member or a graduate teaching assistant may tell a student who has computer skills that unless the student assists in getting unauthorized access to certain data or free computer time, the student will receive a poor or failing grade. Or, a supervising faculty member may tell a graduate student who is trying to finish research needed to complete a dissertation that unless the graduate student helps to break into another faculty member's research database, the faculty supervisor will delay progress on the graduate student's dissertation.

These are unethical and unconscionable pressures. A school or college must deal with them strongly.

ABUSE OF COMPUTERS BY STUDENTS

When a student breaks the code of a computer what should be the institution's response? Should the response to a student's act be different from the response to a faculty or staff member's act?

There are a wide range of responses possible, and it is up to the institution, usually, whether it responds differently to computer abuse done by students compared to that done by faculty or staff.

Breaking the code of a school or college computer is a fairly common activity. Sometimes it is done as a prank, while at other times the breaking of the code may be for some criminal purpose, such as embezzling funds. At still other times, there may be conduct falling somewhere in between, that is, breaking a code in order to change a grade or plagiarize some information or work.

An educational institution has to determine in advance what range of responses it chooses to have available in such situations. It must then make sure to inform students, faculty, staff and others what its policies are regarding computer abuse. If there are potential violations of a state computer crime statute involved, the institution would want to inform students about the statute, what it defines as computer crime, and what the penalties are as to possible imprisonment and fines. Finally, the institution must follow whatever procedures it has said it would follow in instances of computer abuse.

For example, where a student is involved in what is clearly intended as a prank, the institution may wish to respond as it would to other student pranks. At the other extreme, where a student is involved in an activity that clearly is intended as a criminal act, the institution may have little choice but to react much more severely.

An ethical dimension is added to issues of student abuse incidents by the tradition on campus of tending to view a student as a person still going through a learning process, and, therefore, not always being held as accountable as would be the case in some other setting. Exactly how an institution views abuses of computers should be made known to all in advance, as mentioned above. School and college policies and handbooks should make plain which kinds of computer offenses are considered minor offenses and which will be considered serious offenses, and should indicate what different penalties then may be applied. As has just been noted, the intent of the student may make a difference, and could in some instances mitigate the circumstances.

It should be made clear that abuse of computers, however mild, does do some form of damage to computer equipment, data, or other persons, and that some form of punitive response should be expected.

When abuse of computers is the work of nonstudents, such as faculty or other staff members, the same ethical concerns may not apply. Special consideration may be given to students on the basis of the tradition that students are persons still going through a learning process, such that their mistakes may be viewed as part of the learning process. That is not the case with nonstudents. Faculty, staff, and administrators are placed in roles requiring them to supervise students and set examples for students. Therefore, faculty, staff, and administrators often are to be held to a higher standard of behavior than are students.

INSTITUTION'S RESPONSIBILITY TO PROTECT DATA AND RECORDS STORED IN COMPUTERS

A school or college has a responsibility, ethically and legally, to take reasonable steps to protect data and records stored in its computers.

Sometimes it takes no more than a telephone call from a local newspaper reporter to a clerk in an admissions and records office to learn the grades of almost any student there. This has been known to happen regarding inquiries by sports reporters concerning the grades and academic standing of basketball and football players as they relate to eligibility to participate in certain games.

Revealing a student's grades to unauthorized persons is, of course, a violation of the Family Educational Rights and Privacy Act of 1974 (Buckley Amendment) which protects the privacy of students' academic records.

Similarly, a clerk in a personnel office may be asked to reveal certain financial information about faculty or staff salaries to unauthorized persons, such as a bank or a department store.

Such problems usually arise where clerks have not been advised as to what kinds of information may be released, or they have not been given a set of procedures to follow when confronted with such requests.

Generally, supervisors have the responsibility for seeing that security procedures for records and other institutional data and property are developed and followed carefully, including making sure that subordinates have been adequately trained to use the procedures.

ACCESS TO COMPUTERS

Schools and colleges generally have latitude to provide whatever training or access to the use of computers by students and others that they choose. But where training or access is promised it must be delivered.

It is well-established that where, for example, a college catalogue or a person in authority, such as a dean, states that certain courses will include hands-on experience using specific equipment, for instance a computer, there is a contractual obligation to provide such experience. A court ordered the refund of tuition in a case in which a catalogue promised hands-on experience with specific welding equipment, but the equipment was not provided.[1] This is similar to the contractual obligation to provide specific courses, faculty, and facilities set forth in a catalogue.

---

[1] Dizick v. Umpqua Community College, 599 P. 2d 444, Oregon Supreme Court, 1979.

In addition to the contractual obligation described, there also may be an ethical consideration as well. An educational institution may take the position that equity demands that it do its utmost to see that training and access to computers is made available to various of its constituencies. Computer literacy should be available to elementary, secondary, and post-secondary students. At colleges, computer literacy should be accessible not only to its computer science and engineering majors, but to liberal arts majors and others who may be less likely to see, immediately, the importance of computer literacy.

FACULTY EMPLOYMENT AND THE DEVELOPMENT OF COMPUTER PROGRAMS

Legal-ethical issues affect faculty employment. Copyright protection begins from the moment of creation of the work by its author. As mentioned previously, when a faculty member develops a computer program, the question of its ownership arises. The question may be answered by examining the employment relationship between the faculty member and the institution.

If a faculty member is hired specifically to teach computer programming, it well may be that the job description includes an obligation to develop computer programs as part of the normal employment activities expected. In that situation, new computer programs could be considered "works made for hire." The employer, which in this case is the school or college, would be considered to be the "author" of the computer programs, and would own the programs along with the copyright.

If, on the other hand, a faculty member is employed to fulfill the normal duties expected of a faculty person, which at the college level might include teaching, research and service, and the faculty person's discipline is, for instance, biology, then a computer program developed by the faculty person to handle large scale voter surveys probably would not be the property of the institution.

Between the two extremes described above are a great variety of possible scenarios.

What is advisable is that a school or college try to anticipate situations such as those above and others one can imagine easily, and come to some agreement at the time the employment contract is negotiated as to how ownership of intellectual property will be handled.

There are available a number of models of how institutions could handle ownership of intellectual property, such as computer programs. Some examples of models would be:

- the faculty member owns the computer program and licenses it to the institutions for use or marketing;

- the faculty member transfers ownership of the computer program to the institution;
- the institution hired the faculty member to create computer programs, in which case the programs would be deemed to be "works made for hire" and the institution would be considered to be the "author" and owner of the copyright. The institution generally would share royalties in some fashion with the employee who created the program; or
- the institution could commission a faculty member to create a computer program for the institution, and negotiate terms regarding ownership of copyright and sharing of revenues.

From an ethical standpoint, neither the faculty member nor the school or college in such a situation should take undue advantage of the other. Nor should either party wait until the other is at an unexpected disadvantage to bring up the question of ownership of intellectual property.

One example of a situation involving intellectual property arose between a faculty member and a university concerning confidences given to the university by the faculty member relating to his discovery of a secret process. The university claimed sole ownership of the trademark on the secret process. The faculty member alleged there was a fiduciary relationship existent that prevented sole ownership by the university.The lower court held in favor of the faculty member, but the appeals court found in favor of the university. The appeals court said the faculty member had been hired to do the type of research that led to the secret process, so it belonged to the university.[1]

A clear understanding of ownership rights set forth in an employment contract can largely prevent such legal and ethical uncertainties.

ETHICAL RESPONSIBILITIES AT THE INSTITUTIONAL / DEPARTMENTAL / FACULTY LEVEL

A number of ethical issues arise from the fact that private industry is being attracted more and more to educational institutions as resources for research and development activities. Let us suppose that a corporation wishes to provide funds for the support of certain activities within a school or college in connection with the development of computer equipment and programs.

What kind of ethical responsibilities does the institution have to assure that such generosity flowing to certain activities will not deflect the institution from its overall long-range goals? Collegial mechanisms must be utilized to maintain a balance between the opportunities presented for certain localized institutional development and the overall stated mission of the institution.

---

[1] Speck v. North Carolina Dairy Foundation, 319 S.E. 2d 139 (1984).

For example, sometimes specific faculty members are designated as the recipients of industrial funds to do computer-related research. What happens when a faculty person receives substantial amounts of outside funding and is permitted to hire extra secretaries and assistants and to purchase special equipment? What ethical responsibility has the school or college to assure that other members of the department understand that their particular lines of research and areas of interest are still of importance to the institution and the department?

UNKNOWN PHYSICAL DANGERS

A broad ethical concern exists regarding certain physical dangers that are as yet unclear as they relate to computers.

One highly publicized health question is whether video display terminals (VDTs) emit dangerous radiation. This is of concern not only regarding computer operators who work directly in an employer's office, but also where computer operators do an employer's work at home, where not only the employee but the employee's children may be exposed to radiation. A number of studies are being done regarding possible adverse effects of sitting in front of VDTs, but as yet, there are no confirmed health hazards.[1]

From an ethical point of view, what is an employer to do? Should the employer simply take the position that because there are no studies substantially linking VDTs and birth defects, for instance, that there should be no precautions taken with regard to exposing pregnant employees to VDTs? Or, would it be preferable for an employer to allow a pregnant employee to divide her time between the VDT and other work activities during the term of her pregnancy?

What about exposing students to possible harmful effects of VDTs?

Perhaps an institution can devise options that will provide temporary diversions from unproven but possible physical dangers.

RECOMMENDATIONS

Make all reasonable efforts to inform faculty, administrators, staff, and students of institution's position regarding ethical matters.

Clarify the kind of behavior that constitutes infractions of the school or college policies and rules, and what the penalties may be.

Hold regular orientation and training sessions, especially for newcomers.

For further discussion of computer-related ethical issues see:

Hollander, P.A. (1983) University computing facilities: Some ethical dilemmas. In Baca, M.C. and Stein, R.H. (Eds.), *Ethical principles, problems, and practices in higher education.* Springfield, Ill.: C.C. Thomas Publishers.

---

[1] See e.g. The Buffalo News, June 15, 1983, at page C4 at column 1.

Appendix I

Computer Law Glossary

COMPUTER TERMS

Application Software—A specific program written to permit computer user to do his or her own job. Application software often is done by a user's in-house programmer, rather than being supplied by a seller of the system, or by an original equipment manufacturer.

Cathode Ray Tube (CRT)—A TV screen used to display information to the user.

Central Processing Unit (CPU)—This is the actual computing or calculating part of the computer. The entire computer system is usually controlled by the CPU; however, the CPU is transparent to the end-user.

Clean Power— Electric power which has been "filtered" to remove irregularities such as voltage surges and spikes as well as "noise" such as caused by electric motors, etc.

Computer—Result of the memory, input/output (I/O), and central processing unit (CPU) programmed to work together toward an end product.

Computer Assisted Design (CAD)—Consists of computer programmed graphics used in the layout, testing and design of products (usually manufacturing).

Computer Assisted Manufacturing (CAM)—Commonly referred to as robotics, today. Computers are programmed to operate specific manufacturing devices, e.g. to perform certain tasks on an assembly line for the production of automobiles, or in the production of steel.

Cursor—A white square that appears on the cathode ray tube (CRT) to show the user the next position where a character will appear on the screen.

Disk Drive— An input-output device used to store and retrieve programs and operations from inserted magnetic media.

Documentation—Instruction manuals for components of a computing system.

Floppy Disk—Small, flexible and portable, magnetic recording media used in disk drive.

Input-Output (I/O)—Input refers to keyboard, punch cards, or other device that enters data and programs into the central processing unit (CPU). Output refers to a screen , printer, tape, disk, or other device that permits the end product to be retrieved from the CPU.

Main Frame—The largest of the computers manufactured by IBM, Cyber, Cray, and others. Marked by fast CPU operating speed, almost limitless memories and storage, and a large number of users.

Main Memory—Storage place for programs and the data on which the programs operate. Usually consists of RAM Memory (Random Access Memory), supported by ROM (Read Only Memory).

Object Code—The result of compilation or translation of a higher level source code into machine readable language. Object code may be instantly run, or further compiled into machine code.

Memory Pac—Sometimes called Cachet Memory; usually, but not always, ROM (Read Only Memory). Holds specific programs used frequently in processing.

Original Equipment Manufacturer (OEM)—A company that manufactures and sells its own computer products but also buys assembled computer products designed and made by others to resell, often under its own label. An OEM takes on the mantle of the manufacturer.

Peripherals—A general term used to refer to support devices for central processing units and memories. Input-output devices would be referred to as peripherals.

Program—A series of instructions, usually used to manipulate information stored in a memory device. Programs in a computing system are referred to as software, while the electronic and mechanical parts of the system are called hardware.

Random Access Memory (RAM)—A type of memory device that can be both read and written; that is, the user can interact with the RAM.

Read Only Memory (ROM)—A program that is permanent and can be read only; that is, it cannot be changed as can a random access memory (RAM).

Reverse Engineering—The process by which a person who legitimately has acquired a product, such as computer equipment, takes it apart, learns its component parts and operation, and determines how it is designed and manufactured.

Robotics—See Computer Assisted Manufacturing. CAM's that perform tasks in a mechanical, though highly sophisticated, fashion.

The name robotics reflects the fact that many CAM's look like parts of or a complete robot, including, but not always, being able to move about and speak.

Source Code—The highest level of programs. Usually written in languages like Fortran, Basic, Cobol. A computer cannot run source code, so it must be compiled or translated into a usable form for processing. The resulting machine-usable code generally is referred to as object code.

System Software—Basic programming supplied by the manufacturer of the equipment to operate the central processing unit, the memories, and the input-output system.

Terminal—Anything to show the output of the computer; can sometimes be used for the entering of information, if so equipped.

Time-Sharing—A system by which many users may share common access to a computer.

Turnkey Systems—A computing system that is fully operational when powered-on; generally, small minis and micros.

Videotape—Defined under the Copyright Act of 1976 as the reproduction of the images and sounds of a program or programs broadcast by a television broadcast station licensed by the Federal Communications Commission; may be protected by copyright.

LEGAL TERMS

Actual Damages—Money compensation for losses resulting from breach of contract, personal injury, or property damage which readily can be shown to have been sustained and for which the injured party should be compensated as a matter of right.

Breach of Contract—A failure to perform obligations under a contract, and for which failure there is no legal excuse.

Breach of Warranty—A failure to meet the guarantee as to quality, content, condition, or title.

Collateral Estoppel—A doctrine prohibiting the relitigation of issues decided in a prior action.

Consequential Damages—Damages that were reasonably foreseeable as being probable if the contract were broken.

Contract—A set of promises; (1) made by parties competent to contract; (2) regarding a proper subject matter; (3) for proper consideration (such as money); and (4) where there is a mutuality of agreement and obligation. An oral contract is enforceable if it can be performed in less than one year.

Copyright—The protection by federal statute of the original works of authors and artists which gives them the exclusive right to publish their work or determine who may do so.

Copyright Notice—Placing appropriate information on work to inform others regarding ownership, e.g. © 1982 Jane I. Smith.

Copyright Registration—Delivery of work to the U.S. Copyright Office, along with application and fee. Registration generally is required in order for a copyright owner to file suit for infringement of the copyright.

Fair Use—A small amount of copying permitted under the federal copyright law which will not be considered an infringement of a copyright.

First Sale—The first sale doctrine is the principle that a copyright owner loses his exclusive right to sell a particular copy of his work after he parts with the title to that particular copy.

Fixed Work—Under copyright law, a work is "created" when it is "fixed" for the first time. A work is deemed to be "fixed" when it is embodied in a copy or phonorecord or videotape in sufficiently permanent form so as to be perceived or otherwise communicated, such as being reduced to writing or put on tape.

Fraud—An intentional perversion of truth for the purpose of inducing another to rely upon it to part with a valuable thing or surrender a legal right.

Independent Contractor—One who contracts to do work for another according to his own methods and is under his employer's control only as to the result.

Infringement of Copyright—A violation of the exclusive rights of a copyright owner. Remedies for infringement include: injunctions; impounding and disposition of infringing articles; damages and profits; and costs and attorney's fees.

Injunction—A court order to stop or to start a particular act, such as an injunction ordering the cessation of an infringement of copyright.

Lease—An agreement by which one relinquishes his right to immediate possession of property (e.g. a computer) while retaining title. A lease gives exclusive possession of the property against everyone including the owner. A lease must be in writing.

License—A grant of some but not all the rights embraced in a copyright. An agreement giving permission to possess property (e.g. a computer program) and use it subject to the rights of possession of the owner. A license need not be in writing.

Liquidated Damages—An amount of money set forth in a contract which the parties agree will be paid as damages owed to one party if there is a breach of contract by the other.

Negligent Misrepresentation—Negligent refers to an omission to act as a reasonable person under the circumstances. Misrepresentation refers to an untrue statement of fact.

Non-Disclosure Agreement—A promise that certain confidential information (e.g. a trade secret) will not be revealed to others as where an employee agrees not to reveal employer's confidential information, or where a prospective investor or purchaser agrees not to reveal confidential information about a new product.

Patent—Protection of an invention that excludes others from making, selling, or using it during a specified period of time.

Prima Facie Evidence—Evidence that is clear on its face at first view, needing no further explanation.

Privity of Contract—The relationship between two or more contracting parties. It is essential to the maintenance of a legal action on any contract that there be privity of contract between the plaintiff and the defendant in respect to the matter sued on. Requirement of privity is not necessary in the area of products liability.

Products Liability—A doctrine making a manufacturer strictly liable in tort when a product he places in the market, knowing it is to be used without inspection for defects, proves to have a defect that causes injury to a human being.

Proprietary Information—Information belonging to a particular owner, such as a university, a copyright owner, or a company.

Punitive Damages—Compensation in excess of actual damages, meant as a form of punishment and awarded only for willful and malicious misconduct.

Restrictive Employment Agreement—A promise by an employee in exchange for money or other value, that he will not compete with the employer for a certain period of time, in a certain geographic area, doing a certain kind of work.

Restrictive Use Covenant—A promise made as part of a contract that certain property, such as computer programs, will be limited in their use.

Severability—A breach of one clause of a contract would not necessarily mean a breach of all clauses of the contract.

Shop Rights—The right of an employer to use an employee's invention in employer's business without payment of royalties, in effect, a nonexclusive license.

Specific Performance—A requirement that a party guilty of a breach of contract perform the obligations set forth in the contract. Failure to carry out a court decree of specific performance may result in imprisonment for contempt of court.

Statutory Damages—Money compensation set forth in a statute as a remedy for violation of the statute.

Stay—A stopping of a judicial proceeding by order of a court.

Tangible Property—Property capable of being known by the senses, such as real estate or a computer program, as compared with intangible property, such as a copyright or an easement.

Tort—A civil wrong resulting from the violation of a duty. The remedy may be an injunction and/or payment of damages.

Trademark—A word or symbol protected by federal or state statute or by common law from use by others. The term *trademark* refers to a mark used to identify goods, while the term *service mark* refers to a mark used to identify services.

Trade Secret—Information protected by an equitable duty of confidentiality. To prove misappropriation of a trade secret, plaintiff must show (1) plaintiff possessed a trade secret, (2) plaintiff disclosed the trade secret to defendant, (3) plaintiff and defendant shared a confidential relationship, and (4) defendant adopted and used the secret to plaintiff's detriment.—R. Milgrim, *Trade Secrets,* Section 7.07 (1) 1983.

Unfair Competition—The practice of endeavoring to substitute one's own goods or products for those of another, having an established reputation and extensive sale, by means of imitation of name appearance—the imitation being enough to mislead the general public or deceive an unwary customer and yet not amounting to an absolute counterfeit or to the infringement of a trade mark or trade-name—*Singer Mfg. Co. v. June Mfg. Co.,* 163 U.S.169

Warranty, Full—Guaranty as to labor and materials; warrantor must remedy within reasonable time and without charge.

Warranty of Fitness For a Particular Purpose—A guaranty that goods (e.g. computer equipment) are suitable for the special purpose of the buyer, which will not be satisfied by mere fitness for general purposes.

Warranty of Merchantability—A guaranty that the goods (e.g. computer equipment) are reasonably fit for the general purposes for which they are sold.

Appendix II

Checklists

Copyright, Patent, Trade Secret, & Trademark: Some Basic Elements • 78
Acquisition Contracts for Computer Systems • 80
Service Bureau Contracts • 82
Making Copies of Computer Programs—The Legal Perils • 84
"Fair Use" of Computer Programs by Teachers, Scholars, and Researchers • 86
Licensing Computer Software • 88
Employment Contracts re Intellectual Property Rights • 90
Computer Crime Statutes • 92
Insurance for Computers • 98

CHECKLIST—
Copyright, Patent, Trade Secret & Trademark: Some Basic Elements

	Copyright	Patent	Trade Secret	Trademark
What is protected?	Original form of expression of an idea, but not the idea itself. Computer program is copyrightable. See **Apple** v. **Franklin**, 714 **F.**2d 1240, 3rd Cir., 1983.	Novel, non-obvious and useful machine, process, or product. Computer program that is part of a process may be patentable. See **Diamond** v. **Diehr**, 450 **U.S.** 175, 1981.	Both Ideas and expressions; secret information that provides a competitive edge.	Distinctive word or symbol indentifying a product or commodity. (A "service mark" identifies a service.)
What law applies?	Federal: Copyright Act, 17 **U.S.C.** 101.	Federal: Patent Law, 35 **U.S.C.** 101.	State.	Usually federal: Lanham Act, 15 **U.S.C.** 101. State also.
When does protection begin?	Immediately upon being fixed in a tangible form.	When patent is granted.	Immediately.	Upon registration.

Duration of protection:	Life of author plus 50 years (or 75 years).	17 years.	Indefinite, until no longer secret.	20 years, plus renewals.
Form of notice:	Copyright 1984 Jane Doe (may use c in circle).	Patent Pending, or Reg. U.S. Patent Office.		R within a circle.
Cost:	Low ($10 filing fee).	High.	Cost of maintaining secrecy.	Moderate to high.
Remedies available:	Damages, Attorney's fees, Destruction of infringing copies.	Damages, Attorney's fees.	Damages, Attorney's fees.	Damages, Attorney's fees.
Further Information:	U.S. Copyright Office, Library of Congress, Washington, DC 20559 (202) 287-8700.	U.S. Patent and Trademark Office, 2021 Jefferson Davis Highway, Arlington, VA 22202 (703) 557-3158.	State.	U.S. Patent and Trademark Office, 2021 Jefferson Davis Highway, Arlington, VA 22202 (703) 557-3158.

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—*Acquisition Contracts for Computer Systems*

	Yes	No	Action Notes
1. Is the contract written in terms of the *result* expected by the user of the system? e.g.: corporate-level recordkeeping; computer assisted manufacturing; payroll processing; registration of students.)	☐	☐	....
2. Are *hardware* and *software* specified, unit by unit?	☐	☐	....
3. Does the contract incorporate detailed specifications regarding computer system *performance,* such as:			
a. what specific *functions* the supplier says will be done, e.g.: providing numerical and geographical inventory data; printing tabular reports.	☐	☐	....
b. What the *supplier* will do regarding matters such as:			
1. Site preparation;	☐	☐	....
2. Date and method of delivery—penalties for delay;	☐	☐	....
3. Installation;	☐	☐	....
4. Compatibility of Components;	☐	☐	....
5. Documentation;	☐	☐	....
6. Providing personnel;	☐	☐	....
7. Training personnel;	☐	☐	....
8. Testing;	☐	☐	....
9. Guarantees of reliability;	☐	☐	....
10. Security of equipment;	☐	☐	....

11. Confidentiality of user's data; ☐ ☐ ....
12. Maintenance; ☐ ☐ ....
13. Modifications. ☐ ☐ ....

c. What the *user* will do regarding matters such as:

1. Providing clean power; ☐ ☐ ....
2. Providing a proper environment; ☐ ☐ ....
3. Providing qualified staff; ☐ ☐ ....
4. Accepting delivery after testing. ☐ ☐ ....

4. **Financial Matters:**

a. Are rental, purchase, timesharing, or service bureau terms clear, accurate, and mutually understood? ☐ ☐ ....
b. What discounts may apply? ☐ ☐ ....
c. What tax issues should be discussed? ☐ ☐ ....
d. What are the penalties for partial or non-performance? ☐ ☐ ....
e. What backups are there for downtime? ☐ ☐ ....

5. **Insurance:**

a. What coverage is there for damage to, or injury resulting from, equipment or personnel? ☐ ☐ ....
b. What coverage protects the loss of business? ☐ ☐ ....

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—*Service Bureau Contracts*

	Yes	No	Action Notes
1. Does the contract between the user and the service bureau describe exactly the **services** to be performed?	☐	☐	....
e.g., conversion services, developmental services, ongoing services, input processing, report production, production of other items such as payroll checks, testing, correcting errors?	☐	☐	....
2. Is it clear what **hardware, software,** and **personnel** will be used to provide the services?	☐	☐	....
Will the system be available all day, every day, or when?	☐	☐	....
Is the capacity of the system able to handle user's work?	☐	☐	....
How will malfunctions be treated?	☐	☐	....
3. Are there **timetables** for all services?	☐	☐	....
Are there penalties for delays?	☐	☐	....
4. Will service bureau **duplicate user's data?**	☐	☐	....
Will bureau keep duplicates in machine code in fireproof vault off its premises?	☐	☐	....
Will user be given duplicates?	☐	☐	....
5. Are there provisions for disasters?	☐	☐	....
In case of flood, fire, etc., is there another bureau available to handle work?	☐	☐	....
Is there insurance?	☐	☐	....
6. Will the service bureau maintain **confidentiality** of user's data?	☐	☐	....
Will bureau's employees maintain confidentiality?	☐	☐	....

Is it clear that user owns its data and the medium of storage? ☐ ☐ ....

7. What is **user** to do regarding: ☐ ☐ ....
   - Providing accurate data? ☐ ☐ ....
   - Using equipment compatible with that of service bureau? ☐ ☐ ....

8. Is it clear how **costs** are to be calculated? ☐ ☐ ....
   - Will charges be per transaction, flat fee per month, etc? ☐ ☐ ....
   - Are there reduced fees for late services? ☐ ☐ ....
   - Is there a "most favored user" clause? ☐ ☐ ....
   - Are deadlines for payment set forth? ☐ ☐ ....
   - Is there agreement as to who pays taxes? ☐ ☐ ....

9. Are there **warranties** by service bureau? ☐ ☐ ....
   - Does bureau represent that its system is able to perform as promised? ☐ ☐ ....
   - Will bureau indemnify user against third party claims? ☐ ☐ ....

10. Does contract state how contract may be **terminated?** ☐ ☐ ....

11. Does contract set out **remedies?** ☐ ☐ ....
    - Indemnification? ☐ ☐ ....
    - Penalty clauses? ☐ ☐ ....
    - Damages? ☐ ☐ ....

12. Does contract provide for **return to user** of data? ☐ ☐ ....
    - Current source code & documentation? ☐ ☐ ....

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—
Making Copies of Computer Programs—The Legal Perils

The creator of a computer program generally copyrights it in order to protect his or her rights to market it and gain financial benefits from it, among other things.

When another person makes a copy of a computer program that is protected with a valid copyright, without having the permission of the copyright owner, an infringement of the copyright occurs. To avoid infringing copyright, do not make copies of a copyrighted computer program without permission of the copyright owner.

The Copyright Act permits the lawful owner of a copy of a computer program to make one back-up or archival copy, and use a copy of the program in the memory of the computer during its operation. However, if the lawful owner no longer has the right to the copy, (he sells it, for example), the back-up copy must be destroyed. 17 U.S.C. section 117 (1980).

When may the lawful purchaser of a copy of a computer program lawfully make a copy?

Question	*Answer*
When one purchases a computer program, how many copies of it may one make?	One, to serve as a back-up.
May a purchaser make a copy to sell to a friend?	No.
May a purchaser make a copy to give to a friend?	No.
May a business purchaser make a copy to use at home?	No.

May a business purchaser make a copy to use in other computers at work?	No.
Is there any way a purchaser can make more than a back-up copy?	Of course. Get permission of the copyright owner through negotiation.
What are the possible penalties for copyright infringement?	Court order to stop copying. Destruction of copies. Damages. Costs and attorney's fees. Criminal prosecution.

NOTE: In some situations, a person who acquires a computer program may find that he or she is not, in fact, an owner of the computer program, but a licensee. For example, some software is sealed in plastic with a license inside. When the wrapping is torn open, a "tear open" or "shrink wrap" license is said to exist. A licensee is bound by the terms of the license, rather than the provisions of the Copyright Act. The license may not permit even a back-up copy.

There are legal questions about whether a person can become a licensee without knowing about that possibility until opening the package. The legal community cannot speak with assurance about the validity of shrink-wrap licenses until the courts have ruled on the matter. Meantime, many lawyers tend to view that making a back-up copy under such circumstances probably is reasonable, and certainly is prudent. At least one state, Louisiana, is said to be legislating on the validity of shrink-wrap licenses.

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—
"Fair Use" of Computer Programs by Teachers, Scholars, and Researchers

☐ **What is "fair use?"**

Answer: "Fair use" is a legal doctrine that permits copying of computer programs for purposes of teaching, scholarship, and research that otherwise would be deemed an infringement of copyright. The Copyright Act provides that:

"... the fair use of a copyrighted work, ... for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." 17 U.S.C. sec. 107 (1976).

☐ **How does one determine whether any particular use is a "fair use?"**

Answer: The Copyright Act provides that in determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:

(1) "The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;"

(2) "the nature of the copyrighted work;"

(3) "the amount and substantiality of the portion used in relation to the copyrighted work as a whole;" and,

☐ **Does fair use permit copying programs from floppy disks to hard disks?**

Answer: Yes, if the floppy disk is owned and the copy is created as an essential step in utilizing the machine, and for no other purpose.

☐ **Does fair use permit lending a purchased program to students in a serial fashion?**

Answer: Yes, just as one would lend a library book to students in serial fashion.

However, it is not permissible to permit all students to have copies made from the one lawful copy, just as it would not be permissible to make enough copies of a library book so that all students could have copies simultaneously.

☐ **Is it fair use to purchase twenty copies of a program for use by students in one class, and then use the same twenty copies for a subsequent class?**

Answer: Yes. One may purchase and own multiple copies of a computer program and lend them for short periods of time, just as one would do with textbooks. Be sure a back-up copy is made for each purchased copy in case copies lent out are destroyed.

(4) "the effect of the use upon the potential market for or value of the copyrighted work." 17 U.S.C. sec. 107 (1976)

☐ **Does "fair use" permit copying a whole computer program?**

Answer: No, anymore than fair use would permit copying a whole book. (Remember, however, that Sec. 117 of the Copyright Act does permit making one copy or adaptation to be used in the functioning of the machine, i.e. in the memory of the machine, and also permits making one backup copy.)

☐ **Does fair use permit teachers to print the program code to illustrate points in programming classes or prepare derivative works for the same purposes?**

Answer: Probably yes.

☐ **Does fair use permit buying one copy of a computer program and then making twenty more, one for each student's machine?**

Answer: No.

☐ **Suppose students make personal copies from programs lawfully lent to them. Are we liable to the copyright owner for aiding and abetting infringement of copyright?**

Answer: Taking reasonable precautions in the classroom and elsewhere to attempt to prevent unauthorized copying should help counter infringement charges.

☐ **Is there a way to acquire multiple copies of software other than by purchasing them piecemeal?**

Answer: Yes, try to negotiate bulk purchases or persuade software companies to make a tax-favored donation.

☐ **Does the doctrine of fair use apply to software acquired under a license, rather than by a sale?**

Answer: No. The terms of the license control what copies may be made, rather than the terms of the copyright law. Consider negotiating a site license, or try to persuade licensors to donate permission to use the software.

For further discussion of fair use, see Brooks, D.T. (1985) Fair Use of Computer Software by Educators. *EDUCOM Bulletin,* Summer 1985, Vol. 20 No. 2.

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—
Licensing Computer Software

Are you a developer of computer programs, but do not want to use or sell them yourself? You may wish to grant a license to someone else to use or sell the programs you develop in return for a royalty fee.

Do you want to use or sell computer programs, but do not want to develop them yourself? You may wish to pay a royalty fee to secure a license to use or sell programs developed by someone else.

Here are some basic issues to be considered when negotiating a computer software license:

Action Notes

1. What is the **subject matter** of the license?
   - Be specific in defining what is being licensed. Is the license only for the program, or does it include other items such as the object code, system flow charts, operator instructions, and user manuals?
2. What **use** of the licensed material is permitted?
   - Is the use restricted to a specific machine? To a specific room? To a specific building? Is there a set fee for use beyond that stated, or must additional use be negotiated?
3. Are there different royalty arrangements available for different **categories of users**
   - What arrangements are there, for example, for use "in-house" by data processing service providers as compared to licensors who are selling software to others? Such provisions often are referred to as "field-of-user" limitations.
4. What **royalties** will be paid?
   - Is a percentage royalty to be paid on each program? Is there a minimum royalty? What about an advance? When are royalties to be paid? Are royalties due on items other than the program? Are any items free?

5. May **copies** be made?
    - What copies are permissible under the license, in addition to back-up copies? Who owns the copies?

      ....
      ....

6. May **modifications** be made?
    - If so, what provisions are made for removal of the licensed material from the enhanced work, at the time of termination of the license?

      ....
      ....
      ....

7. What provisions are there for maintaining **confidentiality** of the licensed material?
    - Who had access to the licensed material during the term of the license?

      ....
      ....

8. What promises are made regarding date of **delivery**?
    - Is there a penalty for delays?

      ....

9. What constitutes **acceptance** of the specified material?
    - Is the material being delivered all at once, or piecemeal? Is it being tested as it is being installed? What is the meaning of being "operational?"

      ....
      ....
      ....

10. What **warranty** is provided?
    - What liability does the licensor accept, if any, regarding consequential damages?

      ....
      ....

11. What if the licensor goes bankrupt?
    - Has provision been made to place the source code in escrow and keep it updated?

      ....
      ....

12. When and how does the license **terminate**?
    - What materials are to be returned to the licensor?

      ....

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—
Employment Contracts re Intellectual Property Rights

	Yes	No	Action Notes
1. Is there an appropriate set of employment documents, e.g.			
—general employee manual?	☐	☐	....
—individualized employee contracts?	☐	☐	....
—separate non-employee contracts (for consultants, etc.)?	☐	☐	....
2. Does the general employee manual, or other document, set forth:			
a. The employer's general policies regarding intellectual property rights?	☐	☐	....
b. Are copyrights, patents, and trade secrets treated consistently?	☐	☐	....
c. A list of employer's proprietary property—such as copyrights, patents, and trade secrets—that are to be kept confidential and/or are owned by employer?	☐	☐	....
d. A reference to professional standards or ethics to be followed by professional employees?	☐	☐	....
3. Do employee contracts for higher level employees, whose work products are more likely to be deemed work made for hire, contain:			
a. A clear job description, including present and contemplated tasks, so as to avoid questions of "lack of new consideration?"	☐	☐	....
b. A statement of present ownership of intellectual property, such as, that all works are the property of the employer, or that the employer has a right of first refusal?	☐	☐	....

- c. A provision that all works are to be disclosed to the employer, regardless of ownership? ☐ ☐ ....
- d. A non-competition agreement, reasonable as to work, time, and geographic area? ☐ ☐ ....

4. Do employee contracts for lower level employees, whose work products are less likely to be deemed work made for hire, contain:
    - a. An accurate job description? ☐ ☐ ....
    - b. An indication of which ideas and works are property of employer? ☐ ☐ ....
    - c. A provision for transfer of ownership for compensation? ☐ ☐ ....
    - d. A disclosure provision? ☐ ☐ ....

5. Do non-employee contracts (e.g. with consultants) contain:
    - a. A clear definition of the project or task? ☐ ☐ ....
    - b. A statement that the work product is, or is not, to be considered a work made for hire owned by employer? ☐ ☐ ....
    - c. If not a work made for hire, has the consultant agreed to sell the copyright or only the copy? ☐ ☐ ....
    - d. Are patent and trade secrets treated consistently? ☐ ☐ ....
    - e. Is disclosure required? ☐ ☐ ....
    - f. Will ownership be conveyed to employer pending arbitration of scope of employment or reasonableness of royalty if not a work for hire? ☐ ☐ ....
    - g. Does employer have a right of first refusal? ☐ ☐ ....
    - h. If author exercised statutory right to reevaluation, how is risk of error in original valuation handled? ☐ ☐ ....

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—*Computer Crime Statutes*

Information Current as of September, 1984

			PENALTY			
			Imprisonment		Fine	
STATE and STATUTE	CRIME	AMOUNT OF DAMAGE	Min.	Max.	Min.	Max.
ALASKA* §11.46.985	Deceiving a machine (Applies to offenses that require deception as an element, as in theft by deception.)	Less than $50		90 days		$1,000
		$50 - $500		1 year		$5,000
		$500 - $25,000		5 years		$50,000
		More than $25,000		10 years		$50,000
ARIZONA*	Computer fraud, 1st degree (with intent to deceive)			5 years		$150,000
§13-2316	Computer fraud, 2nd degree (Unauthorized access, damage or destruction)			1½ years		$150,000
CALIFORNIA §502	Computer fraud Altering computerized credit information Computer damage or destruction		1 year	*All offenses* 3 years		$10,000
COLORADO* §18-5.5-102	Computer fraud Computer damage or destruction	Less than $50		6 mos.	$50	$750
		$50 - $200	3 mos.	1 year	$250	$1,000
		$200 - $10,000	2 years	4 years		
		More than $10,000	4 years	8 years		
DELAWARE	Computer fraud		2 years	20 years	Individuals; Ct.'s discretion. Corporations; up to $10,000.	
§858	Computer damage or destruction			7 years		

FLORIDA*				
§815.04	Offenses against intellectual property		5 years	$5,000
	With intent to defraud		15 years	$15,000
§815.05	Offenses against computer equipment		1 year	$1,000
	With intent to defraud		5 years	$5,000
	Computer damage or destruction	Less than $200	1 year	$1,000
		$200 - $1,000	5 years	$5,000
		More than $1,000, or causes interruption of gov't or public facility.	15 years	$15,000
§815.06	Offenses against computer users		5 years	$5,000
	With intent to defraud		15 years	$15,000
GEORGIA*				
§16-9-93	Computer fraud		15 years	2½ x the amount of theft
	Computer damage or destruction		15 years	$50,000
ILLINOIS				
ch. 38 §16.9	Unauthorized use of computer	Less than $1,000		$500
	Modification or destruction of programs or data	More than $1,000		$1,000
	Computer fraud	Less than $1,000	1 year	$1,000
		More than $1,000	3 years	Amount of loss or $10,000
MICHIGAN				
			All offenses	
§752.794	Computer fraud	Less than $100	90 days	$100
		More than $100	10 years	$5,000

(*cont. next page*)

STATE and STATUTE	CRIME	AMOUNT OF DAMAGE	PENALTY Imprisonment Min.	PENALTY Imprisonment Max.	PENALTY Fine Min.	PENALTY Fine Max.
MICHIGAN						
§752.795	Computer damage or destruction			*All offenses*		
§752.796	Use of computer to commit: embezzlement; fraudulent disposition of personal property; larceny; larceny by conversion	Less than $100		90 days		$100
		More than $100		10 years		$5,000
MINNESOTA	Computer damage or destruction	Less than $500		90 days		$500
§609.88	Alteration of computer with intent to defraud	$500 - $2,500		5 years		$5,000
		More than $2,500		10 years		$50,000
§609.89	Use of computer in theft	Less than $500		90 days		$500
	Theft of computer	$500 - $2,500		5 years		$5,000
		More than $2,500		10 years		$50,000
MISSOURI						
§569.095	Tampering with intellectual property			1 year		$1,000
	Modification or destruction of computer data					
	Disclosure or theft—trade secrets					
	With intent to defraud	More than $150		5 years	2 x gain to	$20,000
§569.097	Tampering with computer equipment	Less than $150		1 year		$1,000
	With intent to defraud	More than $150		5 years	2 x gain to	$20,000
		More than $1,000, or causes interruption of gov't or public facility		7 years	2 x gain to	$20,000

§569.099	Tampering with computer users (unauthorized access, denial of computer services.)			1 year	$1,000
	With intent to defraud	More than $150		5 years	2 x gain to $20,000
MONTANA					
§45-6-311	Unlawful use of computer (unauthorized use, altering or destroying programs, computer fraud).	Up to $300		6 mos.	$500
		More than $300		10 years	2 x loss to victim
NEW MEXICO					
§30-16A-3	Use of computer to defraud			18 mos.	$5,000
	Use of computer for embezzlement or theft	Less than $100		6 mos.	$500
		$100 - $2,500		18 mos.	$5,000
		More than $2,500		3 years	$5,000
§30-16A-4	Unauthorized computer use	Less than $100		6 mos.	$500
		$100 - $2,500		18 mos.	$5,000
		More than $2,500		3 years	$5,000
NEW YORK					
				All offenses	
(Proposed)	Computer trespass Computer tampering		1 year	4 years	$5,000 or double the profit of computer crime
NORTH CAROLINA					
§14-454	Computer fraud			10 years	Discretionary
§14-455	Damaging computers and related materials			10 years	Discretionary
§14-456	Denial of computer services to authorized user			2 years	Discretionary
§14-457	Extortion via threats to damage computer			10 years	Discretionary

STATE and STATUTE	CRIME	AMOUNT OF DAMAGE	PENALTY Imprisonment Min.		PENALTY Fine Min.	
				Max.		Max.
OHIO						
§2901.01	Expansion of definitions section to include computer-related terms.					
RHODE ISLAND						
§11-52-2	Computer fraud			*All offenses:*		
§11-52-3	Computer damage or destruction	More than $500		5 years		$5,000
§11-52-4	Theft of computer-related materials					
UTAH*				*All Offenses:*		
§76-6-703	Computer fraud Computer damage or destruction	Less than $25		90 days		
		$25 - $100		6 mos.		$299
		$100 - $300		1 year		$1,000
		$300 - $1,000		5 years		$5,000
		More than $1,000		15 years		$10,000
VIRGINIA						
§18.2-152.3	Computer fraud (including embezzlement and larceny)	Less than $200		1 year		$1,000
		More than $200	1 year	10 years	or 1 year /	$1,000
§18.2-152.4	Computer trespass: Removing data; causing malfunction; alter, create or erase data; injure property.			1 year		$1,000
§18.2-152.5	Computer invasion of privacy: (Unauthorized examination of personal or financial data)					$500
§18.2-152.6	Theft of computer services			1 year		$1,000

§18.2-152.7	Personal trespass by computer, cause physical injury:				
	If malicious		5 years	20 years	
	If non-malicious			1 year	$1,000
WISCONSIN §943.70	Offenses against computer data and programs			9 mos.	$10,000
	With intent to defraud			2 years	$10,000
		More than $2,500, or causes interruption of gov't or public facility.		5 years	$10,000
	Offenses against computer equipment and supplies			9 mos.	$10,000
	With intent to defraud			2 years	$10,000
		More than $2,500, or causes interruption of gov't or public facility.		5 years	$10,000

*Alaska: Organizations may be fined the greater of $100,000 or 3 times the gain resulting from the offense.

*Arizona: Sentences of imprisonment may be increased 25% or decreased 50%, depending on circumstances. Organizations may be fined up to $1,000,000.

*Colorado: Depending on the value of the property involved, corporations could be fined either $1,000 - $30,000 or $5,000 - $50,000.

*Florida Fines may be increased up to two times the gain resulting from the offense or loss suffered by the victim.

*Georgia §16-9-95 offers immunity from civil liability to those who report violations of computer crime laws in good faith.

*Utah Depending on the value of the property involved, corporations could be fined from $300 to $10,000.

This checklist is abbreviated in content, and is not meant to be all-inclusive; but is intended to assist readers in developing their own lists relative to their own situations.

CHECKLIST—*Insurance for Computers*

I. COMPUTERS, PROGRAMS AND DATA INSURANCE

Property insurance is available to cover computers, programs,and data. Before selecting a policy, take into account the following issues:

A. Business Computers

1. If your general "all risks" business insurance policy does not protect satisfactorily against accidental damage to computers, ask about special computer insurance policies that are available for computers, terminals, peripherals, programs, data, storage media.
2. Computers are especially vulnerable to damage by moisture, heat, and electrical problems such as surges of power and static electricity, seek the broadest possible coverage, such as protection against:
   - ☐ water
   - ☐ storm damage
   - ☐ floods
   - ☐ fire
   - ☐ explosion
   - ☐ earthquakes
   - ☐ electrical failure
   - ☐ malfunction of other equipment
   - ☐ vandalism
   - ☐ malicious damage
   - ☐ theft
   - ☐ erasure of data by magnet or electricity
3. Does the insurance pay replacement value or depreciated value?
4. Regarding software programs and data, will the insurance pay only to replace blank disks, or will it pay the cost of reentering and or reconstructing the data on the disks?
5. What coverage is available for computers while in transit from one site to another?

V. SOURCES OF COMPUTER INSURANCE COVERAGE:*

Many insurance companies offer protection for computers and computer-related activities. The following list is not meant to be all-inclusive.

- Fireman's Fund
- Hanover
- Hartford
- Kemper
- Ohio Casualty
- Safeco
- Unigard
- United Pacific Reliance

VI. SPECIALIZED COMPUTER INSURANCE POLICIES:

(Partial listing, data subject to change.)

A. **AppleCare,** applications available from authorized Apple dealers.

Apple Computer has fostered AppleCare, a special "all-risk" policy underwritten by the Chubb Group and available through Emett & Chandler, Inc. AppleCare is said to cover one's Apple system, i.e., hardware, software, and accessories, anywhere in the world. AppleCare reportedly covers earthquakes, floods, and electrical and mechanical breakdown, but not programming error or data erasure by magnet or electricity.

Deductible: $100.
Cost: $25 protects system valued to $5000.
$50 to protect up to $25,000.
After premium is paid, any additional equipment bought is covered automatically up to the $25,000 limit at no additional cost.

B. **Safeware.** 2929 North High St., Columbus, OH 43202, (800) 848-3469 or (614) 262-0559.

B. **Home Computers**

1. If computer is used only at home for games & hobbies, not for business purposes at home, will homeowner/renter policy provide protection?
2. What additional premium will be required?
3. If a computer is used at home for business purposes, will it be defined as a ''business machine,'' for which the insurance company will pay only depreciated value, not replacement value?
4. How can one assure that replacement value will be paid?

II. LOSS OF BUSINESS

Does your policy cover loss of business due to interruptions or downtime?

III. PROGRAMMING ERRORS

Consider personal liability insurance to protect programmers or data base owners from claims of material loss resulting from:

☐ errors in a program,
☐ omission of data from program, data base.

IV. INJURY TO PERSONS

Review accident insurance regarding coverage for personal injuries or death caused by:

☐ electrical shock
☐ noxious fumes
☐ leaking radiation
☐ malfunctioning robotic arm

Standard policy does not cover cost of replacing data, but special policy, ''Big Mike'' will, up to $5000.

Deductible: $50
Cost: $35 minimum premium, and $15 increments per $3000 of coverage.
Discounts: for university students at schools requiring use of, and/or having large volume of computer sales to students.

C. **The Personal Computer Insurance Agency**,
P.O. Box 28506, San Jose, CA 95159, (408) 723-8107

Coverage includes damage due to corrosion or air conditioning.

Deductible: None
Cost: Slightly higher premium.
Extra: $10 per month provides ''business interruption'' option paying up to $2500 per month if down at crucial moment.

D. **Data Security Insurance Agency**, 4800 Riverbend Rd., Boulder, CO 80301, (303) 443-3600 (contact company for details).

Note:
In addition to acquiring insurance, remember to make hard copies of all data, and consider getting surge protectors.

---

*Examples of specific insurance companies and policies from: V. Schnatmeier. "Insurance—Protecting Your Computer Investment." In: *A+ Magazine*, November, 1984, p.79.

Appendix III

Copyright Law Amended Regarding Computer Programs

The following excerpt amending title 17, United States Code, is taken from Public Law 96-517, dated December 12, 1980 (94 STAT. 3028-29).

Sec. 10. (a) Section 101 of title 17 of the United States Code is amended to add at the end thereof the following new language:

> "A 'computer program' is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.".

(b) Section 117 of title 17 of the United States Code is amended to read as follows:

"§ 117.[1] Limitations on exclusive rights: Computer programs

"Notwithstanding the provisions of section 106,[2] it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:

> "(1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or
>
> "(2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.

"Any exact copies prepared in accordance with the provisions of this section may be leased, sold, or otherwise transferred, along with the copy from which such copies were prepared, only as part of the lease, sale, or other transfer of all rights in the program. Adaptations so prepared may be transferred only with the authorization of the copyright owner.".

---

[1] 17 USC 117.

[2] 17 USC 106.

Appendix IV

Resources for Legal Information in Secondary and Higher Education

If you have found the information contained in this monograph to be helpful in your day-to-day operations and as a reference it is quite likely that you may also be interested in other titles included in the *The Higher Education Administration Series* or in our publications that offer quarterly updates on case law related to various fields of education.

Following is a list of titles available from College Administration Publications. Where the titles are not illustrative of the subject covered, a brief description is included. If you wish to order, there is an order blank on the reverse side of this sheet which you may wish to copy rather than tearing out this page.

Other titles in *The Higher Education Administration Series:*

- Administering College and University Housing:
  A Legal Perspective
- The Dismissal of Students with Mental Disorders:
  Legal Issues, Policy Considerations
  and Alternative Responses
- Computers in Education:
  Legal Liabilities and Ethical Issues
  Concerning Their Use and Misuse

The following publications offer the reader a quarterly report on recent precedent setting higher court decisions covering a wide range of subjects in the area encompassed by the self-descriptive title. In addition, through the accumulated back issues, and in the "College" publications, a casebook, each of these publications are also excellent comprehensive references that can be of great help in day-to-day operations and long range planning:

- The College Student and the Courts
- The College Administrator and the Courts
- The Schools and the Courts

While primarily written for practicing administrators, superintendents, school boards, teachers and legal counsel in secondary education, this publication is of great value to related schools of education.

Order Blank

Bill to:.............................. *Ship to:*..............................

....

....

Quantity	*Item & Price*	*Total*
______	**The Dismissal of Students with Mental Disorders:** 1 to 9 copies @ $9.95; 10 or more copies @ $9.50	______
______	**Administering College and University Housing:** 1 to 9 copies @ $9.95; 10 or more copies @ $9.50	______
______	**A Practical Guide to Legal Issues Affecting College Teachers** 1 to 9 copies @ $4.95; 10 to 24 copies @ $3.95; 25 or more copies @ $3.50	______
______	**Computers in Education: Legal Liabilities and Ethical Issues Concerning Their Use and Misuse** 1 to 9 copies @ $9.95; 10 or more copies @ $9.50	______
______	**The College Student and the Courts** Includes casebook, all back issues and four quarterly updating supplements..............$98.50	______
______	**The College Administrator and the Courts** Includes casebook, all back issues and four quarterly updating supplements..............$77.50	______
______	**The Schools and the Courts** Includes over 600 pages of back issues and four updating reports...........................$67.50	______
	Postage (if payment accompanies order we will ship postpaid)	______
	North Carolina residents add appropriate sales tax	______
	Total	______

Address Orders to:

College Administration Publications, Inc.
Dept. CM, P.O. Box 8492, Asheville, NC 28814

☐ Pricing of the above publications was correct on the publication date of this monograph. If you wish to be advised of current prices of titles you have ordered before shipment, please check.

☐ For further information regarding any of the above titles please indicate with check here and in the quantity column of each publication and we will forward current brochures and information.

DETACH AND MAIL